



Guía de referencia

AWS Política gestionada



AWS Política gestionada: Guía de referencia

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

Las marcas registradas y la imagen comercial de Amazon no se pueden utilizar en ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, relacionados o patrocinados por Amazon.

Table of Contents

| | |
|---|----|
| ¿Qué son las políticas administradas por AWS? | 1 |
| Descripción de las páginas de referencia de las políticas | 1 |
| Políticas obsoletas administradas por AWS | 2 |
| AWS políticas gestionadas | 3 |
| AccessAnalyzerServiceRolePolicy | 43 |
| Uso de esta política | 43 |
| Información de la política | 43 |
| Versión de la política | 43 |
| Documento de política JSON | 44 |
| Más información | 46 |
| AdministratorAccess | 46 |
| Uso de la política | 46 |
| Información de la política | 46 |
| Versión de la política | 46 |
| Documento de política JSON | 47 |
| Más información | 47 |
| AdministratorAccess-Amplify | 47 |
| Uso de esta política | 47 |
| Detalles de la política | 48 |
| Versión de la política | 48 |
| Documento de política JSON | 48 |
| Más información | 58 |
| AdministratorAccess-AWSElasticBeanstalk | 59 |
| Uso de esta política | 59 |
| Detalles de la política | 59 |
| Versión de la política | 59 |
| Documento de política JSON | 59 |
| Más información | 67 |
| AlexaForBusinessDeviceSetup | 68 |
| Uso de esta política | 68 |
| Detalles de la política | 68 |
| Versión de la política | 68 |
| Documento de política JSON | 68 |
| Más información | 69 |

| | |
|---|----|
| AlexaForBusinessFullAccess | 69 |
| Uso de esta política | 69 |
| Detalles de la política | 69 |
| Versión de la política | 70 |
| Documento de política JSON | 70 |
| Más información | 71 |
| AlexaForBusinessGatewayExecution | 72 |
| Uso de esta política | 72 |
| Detalles de la política | 72 |
| Versión de la política | 72 |
| Documento de política JSON | 72 |
| Más información | 73 |
| AlexaForBusinessLifesizeDelegatedAccessPolicy | 73 |
| Uso de esta política | 73 |
| Detalles de la política | 74 |
| Versión de la política | 74 |
| Documento de política JSON | 74 |
| Más información | 76 |
| AlexaForBusinessNetworkProfileServicePolicy | 77 |
| Uso de esta política | 77 |
| Detalles de la política | 77 |
| Versión de la política | 77 |
| Documento de política JSON | 77 |
| Más información | 78 |
| AlexaForBusinessPolyDelegatedAccessPolicy | 78 |
| Uso de esta política | 78 |
| Detalles de la política | 78 |
| Versión de la política | 79 |
| Documento de política JSON | 79 |
| Más información | 81 |
| AlexaForBusinessReadOnlyAccess | 81 |
| Uso de esta política | 81 |
| Detalles de la política | 81 |
| Versión de la política | 81 |
| Documento de política JSON | 81 |
| Más información | 82 |

| | |
|--|----|
| AmazonAPIGatewayAdministrator | 82 |
| Uso de esta política | 82 |
| Detalles de la política | 82 |
| Versión de la política | 83 |
| Documento de política JSON | 83 |
| Más información | 83 |
| AmazonAPIGatewayInvokeFullAccess | 83 |
| Uso de esta política | 84 |
| Detalles de la política | 84 |
| Versión de la política | 84 |
| Documento de política JSON | 84 |
| Más información | 84 |
| AmazonAPIGatewayPushToCloudWatchLogs | 85 |
| Uso de esta política | 85 |
| Detalles de la política | 85 |
| Versión de la política | 85 |
| Documento de política JSON | 85 |
| Más información | 86 |
| AmazonAppFlowFullAccess | 86 |
| Uso de esta política | 86 |
| Detalles de la política | 86 |
| Versión de la política | 87 |
| Documento de política JSON | 87 |
| Más información | 90 |
| AmazonAppFlowReadOnlyAccess | 90 |
| Uso de esta política | 90 |
| Detalles de la política | 90 |
| Versión de la política | 90 |
| Documento de política JSON | 90 |
| Más información | 91 |
| AmazonAppStreamFullAccess | 91 |
| Uso de esta política | 91 |
| Detalles de la política | 91 |
| Versión de la política | 92 |
| Documento de política JSON | 92 |
| Más información | 94 |

| | |
|--|-----|
| AmazonAppStreamPCAAccess | 94 |
| Uso de esta política | 94 |
| Detalles de la política | 94 |
| Versión de la política | 94 |
| Documento de política JSON | 95 |
| Más información | 95 |
| AmazonAppStreamReadOnlyAccess | 95 |
| Uso de esta política | 95 |
| Detalles de la política | 96 |
| Versión de la política | 96 |
| Documento de política JSON | 96 |
| Más información | 96 |
| AmazonAppStreamServiceAccess | 97 |
| Uso de esta política | 97 |
| Detalles de la política | 97 |
| Versión de la política | 97 |
| Documento de política JSON | 97 |
| Más información | 98 |
| AmazonAthenaFullAccess | 99 |
| Uso de esta política | 99 |
| Información de la política | 99 |
| Versión de la política | 99 |
| Documento de política JSON | 99 |
| Más información | 103 |
| AmazonAugmentedAIFullAccess | 103 |
| Uso de esta política | 103 |
| Detalles de la política | 103 |
| Versión de la política | 103 |
| Documento de política JSON | 104 |
| Más información | 105 |
| AmazonAugmentedAIHumanLoopFullAccess | 105 |
| Uso de esta política | 105 |
| Detalles de la política | 105 |
| Versión de la política | 105 |
| Documento de política JSON | 105 |
| Más información | 106 |

| | |
|---|-----|
| AmazonAugmentedAllIntegratedAPIAccess | 106 |
| Uso de esta política | 106 |
| Detalles de la política | 106 |
| Versión de la política | 107 |
| Documento de política JSON | 107 |
| Más información | 108 |
| AmazonBedrockFullAccess | 108 |
| Uso de la política | 109 |
| Información de la política | 109 |
| Versión de la política | 109 |
| Documento de política JSON | 109 |
| Más información | 110 |
| AmazonBedrockReadOnly | 111 |
| Uso de la política | 111 |
| Información de la política | 111 |
| Versión de la política | 111 |
| Documento de política JSON | 111 |
| Más información | 112 |
| AmazonBraketFullAccess | 112 |
| Uso de esta política | 112 |
| Detalles de la política | 112 |
| Versión de la política | 113 |
| Documento de política JSON | 113 |
| Más información | 117 |
| AmazonBraketJobsExecutionPolicy | 117 |
| Uso de esta política | 117 |
| Detalles de la política | 117 |
| Versión de la política | 118 |
| Documento de política JSON | 118 |
| Más información | 120 |
| AmazonBraketServiceRolePolicy | 121 |
| Uso de esta política | 121 |
| Detalles de la política | 121 |
| Versión de la política | 121 |
| Documento de política JSON | 121 |
| Más información | 122 |

| | |
|---|-----|
| AmazonChimeFullAccess | 122 |
| Uso de esta política | 122 |
| Detalles de la política | 122 |
| Versión de la política | 123 |
| Documento de política JSON | 123 |
| Más información | 125 |
| AmazonChimeReadOnly | 125 |
| Uso de esta política | 125 |
| Detalles de la política | 125 |
| Versión de la política | 126 |
| Documento de política JSON | 126 |
| Más información | 126 |
| AmazonChimeSDK | 126 |
| Uso de esta política | 127 |
| Detalles de la política | 127 |
| Versión de la política | 127 |
| Documento de política JSON | 127 |
| Más información | 128 |
| AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy | 128 |
| Uso de la política | 129 |
| Información de la política | 129 |
| Versión de la política | 129 |
| Documento de política JSON | 129 |
| Más información | 130 |
| AmazonChimeSDKMessagingServiceRolePolicy | 131 |
| Uso de esta política | 131 |
| Detalles de la política | 131 |
| Versión de la política | 131 |
| Documento de política JSON | 131 |
| Más información | 132 |
| AmazonChimeServiceRolePolicy | 132 |
| Uso de esta política | 132 |
| Detalles de la política | 132 |
| Versión de la política | 133 |
| Documento de política JSON | 133 |
| Más información | 133 |

| | |
|--|-----|
| AmazonChimeTranscriptionServiceLinkedRolePolicy | 134 |
| Uso de esta política | 134 |
| Detalles de la política | 134 |
| Versión de la política | 134 |
| Documento de política JSON | 134 |
| Más información | 135 |
| AmazonChimeUserManagement | 135 |
| Uso de esta política | 135 |
| Detalles de la política | 135 |
| Versión de la política | 135 |
| Documento de política JSON | 136 |
| Más información | 137 |
| AmazonChimeVoiceConnectorServiceLinkedRolePolicy | 137 |
| Uso de esta política | 137 |
| Detalles de la política | 137 |
| Versión de la política | 138 |
| Documento de política JSON | 138 |
| Más información | 140 |
| AmazonCloudDirectoryFullAccess | 140 |
| Uso de esta política | 140 |
| Detalles de la política | 140 |
| Versión de la política | 140 |
| Documento de política JSON | 140 |
| Más información | 141 |
| AmazonCloudDirectoryReadOnlyAccess | 141 |
| Uso de esta política | 141 |
| Detalles de la política | 141 |
| Versión de la política | 141 |
| Documento de política JSON | 142 |
| Más información | 142 |
| AmazonCloudWatchEvidentlyFullAccess | 142 |
| Uso de esta política | 143 |
| Detalles de la política | 143 |
| Versión de la política | 143 |
| Documento de política JSON | 143 |
| Más información | 146 |

| | |
|--|-----|
| AmazonCloudWatchEvidentlyReadOnlyAccess | 146 |
| Uso de esta política | 146 |
| Detalles de la política | 146 |
| Versión de la política | 146 |
| Documento de política JSON | 146 |
| Más información | 147 |
| AmazonCloudWatchEvidentlyServiceRolePolicy | 147 |
| Uso de esta política | 147 |
| Detalles de la política | 148 |
| Versión de la política | 148 |
| Documento de política JSON | 148 |
| Más información | 149 |
| AmazonCloudWatchRUMFullAccess | 150 |
| Uso de esta política | 150 |
| Detalles de la política | 150 |
| Versión de la política | 150 |
| Documento de política JSON | 150 |
| Más información | 153 |
| AmazonCloudWatchRUMReadOnlyAccess | 153 |
| Uso de esta política | 153 |
| Detalles de la política | 153 |
| Versión de la política | 153 |
| Documento de política JSON | 154 |
| Más información | 154 |
| AmazonCloudWatchRUMServiceRolePolicy | 154 |
| Uso de esta política | 154 |
| Detalles de la política | 155 |
| Versión de la política | 155 |
| Documento de política JSON | 155 |
| Más información | 156 |
| AmazonCodeCatalystFullAccess | 156 |
| Uso de esta política | 156 |
| Detalles de la política | 156 |
| Versión de la política | 156 |
| Documento de política JSON | 157 |
| Más información | 157 |

| | |
|--|-----|
| AmazonCodeCatalystReadOnlyAccess | 158 |
| Uso de esta política | 158 |
| Detalles de la política | 158 |
| Versión de la política | 158 |
| Documento de política JSON | 158 |
| Más información | 159 |
| AmazonCodeCatalystSupportAccess | 159 |
| Uso de esta política | 159 |
| Detalles de la política | 159 |
| Versión de la política | 159 |
| Documento de política JSON | 159 |
| Más información | 160 |
| AmazonCodeGuruProfilerAgentAccess | 160 |
| Uso de esta política | 161 |
| Detalles de la política | 161 |
| Versión de la política | 161 |
| Documento de política JSON | 161 |
| Más información | 162 |
| AmazonCodeGuruProfilerFullAccess | 162 |
| Uso de esta política | 162 |
| Detalles de la política | 162 |
| Versión de la política | 162 |
| Documento de política JSON | 162 |
| Más información | 163 |
| AmazonCodeGuruProfilerReadOnlyAccess | 163 |
| Uso de esta política | 164 |
| Detalles de la política | 164 |
| Versión de la política | 164 |
| Documento de política JSON | 164 |
| Más información | 165 |
| AmazonCodeGuruReviewerFullAccess | 165 |
| Uso de esta política | 165 |
| Detalles de la política | 165 |
| Versión de la política | 165 |
| Documento de política JSON | 165 |
| Más información | 168 |

| | |
|---|-----|
| AmazonCodeGuruReviewerReadOnlyAccess | 168 |
| Uso de esta política | 168 |
| Detalles de la política | 168 |
| Versión de la política | 169 |
| Documento de política JSON | 169 |
| Más información | 169 |
| AmazonCodeGuruReviewerServiceRolePolicy | 170 |
| Uso de esta política | 170 |
| Detalles de la política | 170 |
| Versión de la política | 170 |
| Documento de política JSON | 170 |
| Más información | 172 |
| AmazonCodeGuruSecurityFullAccess | 172 |
| Uso de esta política | 173 |
| Detalles de la política | 173 |
| Versión de la política | 173 |
| Documento de política JSON | 173 |
| Más información | 173 |
| AmazonCodeGuruSecurityScanAccess | 174 |
| Uso de esta política | 174 |
| Detalles de la política | 174 |
| Versión de la política | 174 |
| Documento de política JSON | 174 |
| Más información | 175 |
| AmazonCognitoDeveloperAuthenticatedIdentities | 175 |
| Uso de esta política | 175 |
| Detalles de la política | 175 |
| Versión de la política | 176 |
| Documento de política JSON | 176 |
| Más información | 176 |
| AmazonCognitoIdpEmailServiceRolePolicy | 177 |
| Uso de esta política | 177 |
| Detalles de la política | 177 |
| Versión de la política | 177 |
| Documento de política JSON | 177 |
| Más información | 178 |

| | |
|--|-----|
| AmazonCognitoIdpServiceRolePolicy | 178 |
| Uso de esta política | 178 |
| Detalles de la política | 178 |
| Versión de la política | 179 |
| Documento de política JSON | 179 |
| Más información | 179 |
| AmazonCognitoPowerUser | 179 |
| Uso de esta política | 179 |
| Detalles de la política | 180 |
| Versión de la política | 180 |
| Documento de política JSON | 180 |
| Más información | 181 |
| AmazonCognitoReadOnly | 182 |
| Uso de esta política | 182 |
| Detalles de la política | 182 |
| Versión de la política | 182 |
| Documento de política JSON | 182 |
| Más información | 183 |
| AmazonCognitoUnAuthedIdentitiesSessionPolicy | 183 |
| Uso de esta política | 183 |
| Detalles de la política | 184 |
| Versión de la política | 184 |
| Documento de política JSON | 184 |
| Más información | 185 |
| AmazonCognitoUnauthenticatedIdentities | 185 |
| Uso de esta política | 185 |
| Detalles de la política | 185 |
| Versión de la política | 185 |
| Documento de política JSON | 186 |
| Más información | 186 |
| AmazonConnect_FullAccess | 186 |
| Uso de esta política | 186 |
| Detalles de la política | 187 |
| Versión de la política | 187 |
| Documento de política JSON | 187 |
| Más información | 190 |

| | |
|---|-----|
| AmazonConnectCampaignsServiceLinkedRolePolicy | 190 |
| Uso de esta política | 190 |
| Información de la política | 190 |
| Versión de la política | 190 |
| Documento de política JSON | 191 |
| Más información | 191 |
| AmazonConnectReadOnlyAccess | 191 |
| Uso de esta política | 191 |
| Detalles de la política | 192 |
| Versión de la política | 192 |
| Documento de política JSON | 192 |
| Más información | 193 |
| AmazonConnectServiceLinkedRolePolicy | 193 |
| Uso de esta política | 193 |
| Información de la política | 193 |
| Versión de la política | 193 |
| Documento de política JSON | 194 |
| Más información | 198 |
| AmazonConnectSynchronizationServiceRolePolicy | 198 |
| Uso de esta política | 199 |
| Detalles de la política | 199 |
| Versión de la política | 199 |
| Documento de política JSON | 199 |
| Más información | 201 |
| AmazonConnectVoiceIDFullAccess | 201 |
| Uso de esta política | 201 |
| Detalles de la política | 201 |
| Versión de la política | 202 |
| Documento de política JSON | 202 |
| Más información | 202 |
| AmazonDataZoneDomainExecutionRolePolicy | 203 |
| Uso de la política | 203 |
| Información de la política | 203 |
| Versión de la política | 203 |
| Documento de política JSON | 203 |
| Más información | 206 |

| | |
|--|-----|
| AmazonDataZoneEnvironmentRolePermissionsBoundary | 206 |
| Uso de la política | 206 |
| Información de la política | 207 |
| Versión de la política | 207 |
| Documento de política JSON | 207 |
| Más información | 220 |
| AmazonDataZoneFullAccess | 220 |
| Uso de la política | 220 |
| Información de la política | 220 |
| Versión de la política | 221 |
| Documento de política JSON | 221 |
| Más información | 224 |
| AmazonDataZoneFullUserAccess | 224 |
| Uso de la política | 224 |
| Información de la política | 224 |
| Versión de la política | 225 |
| Documento de política JSON | 225 |
| Más información | 228 |
| AmazonDataZoneGlueManageAccessRolePolicy | 228 |
| Uso de la política | 228 |
| Información de la política | 228 |
| Versión de la política | 228 |
| Documento de política JSON | 229 |
| Más información | 232 |
| AmazonDataZonePortalFullAccessPolicy | 232 |
| Uso de esta política | 232 |
| Detalles de la política | 233 |
| Versión de la política | 233 |
| Documento de política JSON | 233 |
| Más información | 233 |
| AmazonDataZonePreviewConsoleFullAccess | 234 |
| Uso de esta política | 234 |
| Detalles de la política | 234 |
| Versión de la política | 234 |
| Documento de política JSON | 234 |
| Más información | 236 |

| | |
|--|-----|
| AmazonDataZoneProjectDeploymentPermissionsBoundary | 236 |
| Uso de esta política | 236 |
| Detalles de la política | 237 |
| Versión de la política | 237 |
| Documento de política JSON | 237 |
| Más información | 245 |
| AmazonDataZoneProjectRolePermissionsBoundary | 245 |
| Uso de esta política | 245 |
| Detalles de la política | 245 |
| Versión de la política | 246 |
| Documento de política JSON | 246 |
| Más información | 253 |
| AmazonDataZoneRedshiftGlueProvisioningPolicy | 253 |
| Uso de la política | 254 |
| Información de la política | 254 |
| Versión de la política | 254 |
| Documento de política JSON | 254 |
| Más información | 262 |
| AmazonDataZoneRedshiftManageAccessRolePolicy | 262 |
| Uso de la política | 262 |
| Información de la política | 262 |
| Versión de la política | 263 |
| Documento de política JSON | 263 |
| Más información | 265 |
| AmazonDetectiveFullAccess | 265 |
| Uso de esta política | 265 |
| Detalles de la política | 265 |
| Versión de la política | 266 |
| Documento de política JSON | 266 |
| Más información | 267 |
| AmazonDetectiveInvestigatorAccess | 267 |
| Uso de esta política | 267 |
| Información de la política | 267 |
| Versión de la política | 267 |
| Documento de política JSON | 268 |
| Más información | 269 |

| | |
|--|-----|
| AmazonDetectiveMemberAccess | 269 |
| Uso de esta política | 270 |
| Detalles de la política | 270 |
| Versión de la política | 270 |
| Documento de política JSON | 270 |
| Más información | 271 |
| AmazonDetectiveOrganizationsAccess | 271 |
| Uso de esta política | 271 |
| Detalles de la política | 271 |
| Versión de la política | 271 |
| Documento de política JSON | 272 |
| Más información | 273 |
| AmazonDetectiveServiceLinkedRolePolicy | 274 |
| Uso de esta política | 274 |
| Detalles de la política | 274 |
| Versión de la política | 274 |
| Documento de política JSON | 274 |
| Más información | 275 |
| AmazonDevOpsGuruConsoleFullAccess | 275 |
| Uso de esta política | 275 |
| Detalles de la política | 275 |
| Versión de la política | 275 |
| Documento de política JSON | 275 |
| Más información | 278 |
| AmazonDevOpsGuruFullAccess | 278 |
| Uso de esta política | 278 |
| Detalles de la política | 278 |
| Versión de la política | 279 |
| Documento de política JSON | 279 |
| Más información | 281 |
| AmazonDevOpsGuruOrganizationsAccess | 281 |
| Uso de esta política | 281 |
| Detalles de la política | 281 |
| Versión de la política | 282 |
| Documento de política JSON | 282 |
| Más información | 283 |

| | |
|--|-----|
| AmazonDevOpsGuruReadOnlyAccess | 283 |
| Uso de esta política | 283 |
| Detalles de la política | 284 |
| Versión de la política | 284 |
| Documento de política JSON | 284 |
| Más información | 286 |
| AmazonDevOpsGuruServiceRolePolicy | 286 |
| Uso de esta política | 286 |
| Detalles de la política | 286 |
| Versión de la política | 287 |
| Documento de política JSON | 287 |
| Más información | 291 |
| AmazonDMSCloudWatchLogsRole | 291 |
| Uso de esta política | 291 |
| Detalles de la política | 291 |
| Versión de la política | 291 |
| Documento de política JSON | 292 |
| Más información | 293 |
| AmazonDMSRedshiftS3Role | 293 |
| Uso de esta política | 293 |
| Detalles de la política | 294 |
| Versión de la política | 294 |
| Documento de política JSON | 294 |
| Más información | 295 |
| AmazonDMSVPCManagementRole | 295 |
| Uso de esta política | 295 |
| Detalles de la política | 295 |
| Versión de la política | 295 |
| Documento de política JSON | 296 |
| Más información | 296 |
| AmazonDocDB-ElasticServiceRolePolicy | 296 |
| Uso de esta política | 297 |
| Detalles de la política | 297 |
| Versión de la política | 297 |
| Documento de política JSON | 297 |
| Más información | 298 |

| | |
|--|-----|
| AmazonDocDBConsoleFullAccess | 298 |
| Uso de esta política | 298 |
| Detalles de la política | 298 |
| Versión de la política | 298 |
| Documento de política JSON | 299 |
| Más información | 303 |
| AmazonDocDBElasticFullAccess | 303 |
| Uso de esta política | 303 |
| Detalles de la política | 303 |
| Versión de la política | 303 |
| Documento de política JSON | 304 |
| Más información | 307 |
| AmazonDocDBElasticReadOnlyAccess | 307 |
| Uso de esta política | 307 |
| Detalles de la política | 307 |
| Versión de la política | 307 |
| Documento de política JSON | 307 |
| Más información | 308 |
| AmazonDocDBFullAccess | 308 |
| Uso de esta política | 309 |
| Detalles de la política | 309 |
| Versión de la política | 309 |
| Documento de política JSON | 309 |
| Más información | 312 |
| AmazonDocDBReadOnlyAccess | 312 |
| Uso de esta política | 312 |
| Detalles de la política | 312 |
| Versión de la política | 312 |
| Documento de política JSON | 313 |
| Más información | 314 |
| AmazonDRSVPCManagement | 315 |
| Uso de esta política | 315 |
| Detalles de la política | 315 |
| Versión de la política | 315 |
| Documento de política JSON | 315 |
| Más información | 316 |

| | |
|--|-----|
| AmazonDynamoDBFullAccess | 316 |
| Uso de esta política | 316 |
| Detalles de la política | 316 |
| Versión de la política | 317 |
| Documento de política JSON | 317 |
| Más información | 319 |
| AmazonDynamoDBFullAccesswithDataPipeline | 320 |
| Uso de esta política | 320 |
| Detalles de la política | 320 |
| Versión de la política | 320 |
| Documento de política JSON | 320 |
| Más información | 322 |
| AmazonDynamoDBReadOnlyAccess | 323 |
| Uso de la política | 323 |
| Información de la política | 323 |
| Versión de la política | 323 |
| Documento de política JSON | 323 |
| Más información | 325 |
| AmazonEBSCSIDriverPolicy | 325 |
| Uso de esta política | 325 |
| Detalles de la política | 325 |
| Versión de la política | 326 |
| Documento de política JSON | 326 |
| Más información | 329 |
| AmazonEC2ContainerRegistryFullAccess | 329 |
| Uso de esta política | 329 |
| Detalles de la política | 329 |
| Versión de la política | 330 |
| Documento de política JSON | 330 |
| Más información | 330 |
| AmazonEC2ContainerRegistryPowerUser | 331 |
| Uso de esta política | 331 |
| Detalles de la política | 331 |
| Versión de la política | 331 |
| Documento de política JSON | 331 |
| Más información | 332 |

| | |
|--|-----|
| AmazonEC2ContainerRegistryReadOnly | 332 |
| Uso de esta política | 332 |
| Detalles de la política | 333 |
| Versión de la política | 333 |
| Documento de política JSON | 333 |
| Más información | 334 |
| AmazonEC2ContainerServiceAutoscaleRole | 334 |
| Uso de esta política | 334 |
| Detalles de la política | 334 |
| Versión de la política | 334 |
| Documento de política JSON | 334 |
| Más información | 335 |
| AmazonEC2ContainerServiceEventsRole | 335 |
| Uso de esta política | 336 |
| Detalles de la política | 336 |
| Versión de la política | 336 |
| Documento de política JSON | 336 |
| Más información | 337 |
| AmazonEC2ContainerServiceforEC2Role | 337 |
| Uso de esta política | 337 |
| Detalles de la política | 338 |
| Versión de la política | 338 |
| Documento de política JSON | 338 |
| Más información | 339 |
| AmazonEC2ContainerServiceRole | 339 |
| Uso de esta política | 339 |
| Detalles de la política | 339 |
| Versión de la política | 340 |
| Documento de política JSON | 340 |
| Más información | 340 |
| AmazonEC2FullAccess | 341 |
| Uso de esta política | 341 |
| Detalles de la política | 341 |
| Versión de la política | 341 |
| Documento de política JSON | 341 |
| Más información | 342 |

| | |
|--|-----|
| AmazonEC2ReadOnlyAccess | 343 |
| Uso de la política | 343 |
| Información de la política | 343 |
| Versión de la política | 343 |
| Documento de política JSON | 343 |
| Más información | 344 |
| AmazonEC2RoleforAWSCodeDeploy | 344 |
| Uso de esta política | 344 |
| Detalles de la política | 344 |
| Versión de la política | 345 |
| Documento de política JSON | 345 |
| Más información | 345 |
| AmazonEC2RoleforAWSCodeDeployLimited | 346 |
| Uso de esta política | 346 |
| Detalles de la política | 346 |
| Versión de la política | 346 |
| Documento de política JSON | 346 |
| Más información | 347 |
| AmazonEC2RoleforDataPipelineRole | 347 |
| Uso de esta política | 347 |
| Detalles de la política | 347 |
| Versión de la política | 348 |
| Documento de política JSON | 348 |
| Más información | 349 |
| AmazonEC2RoleforSSM | 349 |
| Uso de esta política | 349 |
| Detalles de la política | 349 |
| Versión de la política | 349 |
| Documento de política JSON | 350 |
| Más información | 352 |
| AmazonEC2RolePolicyForLaunchWizard | 352 |
| Uso de esta política | 352 |
| Detalles de la política | 352 |
| Versión de la política | 353 |
| Documento de política JSON | 353 |
| Más información | 357 |

| | |
|--|-----|
| AmazonEC2SpotFleetAutoscaleRole | 357 |
| Uso de esta política | 357 |
| Detalles de la política | 357 |
| Versión de la política | 357 |
| Documento de política JSON | 358 |
| Más información | 359 |
| AmazonEC2SpotFleetTaggingRole | 359 |
| Uso de esta política | 359 |
| Detalles de la política | 359 |
| Versión de la política | 359 |
| Documento de política JSON | 359 |
| Más información | 361 |
| AmazonECS_FullAccess | 361 |
| Uso de esta política | 361 |
| Detalles de la política | 361 |
| Versión de la política | 362 |
| Documento de política JSON | 362 |
| Más información | 367 |
| AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity | 367 |
| Uso de la política | 368 |
| Información de la política | 368 |
| Versión de la política | 368 |
| Documento de política JSON | 368 |
| Más información | 370 |
| AmazonECSInfrastructureRolePolicyForVolumes | 371 |
| Uso de la política | 371 |
| Información de la política | 371 |
| Versión de la política | 371 |
| Documento de política JSON | 371 |
| Más información | 373 |
| AmazonECSServiceRolePolicy | 373 |
| Uso de esta política | 374 |
| Información de la política | 374 |
| Versión de la política | 374 |
| Documento de política JSON | 374 |
| Más información | 379 |

| | |
|--|-----|
| AmazonECSTaskExecutionRolePolicy | 379 |
| Uso de esta política | 379 |
| Detalles de la política | 379 |
| Versión de la política | 379 |
| Documento de política JSON | 380 |
| Más información | 380 |
| AmazonEFSCSIDriverPolicy | 380 |
| Uso de esta política | 381 |
| Detalles de la política | 381 |
| Versión de la política | 381 |
| Documento de política JSON | 381 |
| Más información | 383 |
| AmazonEKS_CNI_Policy | 383 |
| Uso de la política | 383 |
| Información de la política | 383 |
| Versión de la política | 383 |
| Documento de política JSON | 384 |
| Más información | 384 |
| AmazonEKSClusterPolicy | 385 |
| Uso de esta política | 385 |
| Detalles de la política | 385 |
| Versión de la política | 385 |
| Documento de política JSON | 385 |
| Más información | 387 |
| AmazonEKSClusterConnectorServiceRolePolicy | 388 |
| Uso de esta política | 388 |
| Detalles de la política | 388 |
| Versión de la política | 388 |
| Documento de política JSON | 388 |
| Más información | 390 |
| AmazonEKSFargatePodExecutionRolePolicy | 390 |
| Uso de esta política | 390 |
| Detalles de la política | 390 |
| Versión de la política | 391 |
| Documento de política JSON | 391 |
| Más información | 391 |

| | |
|--|-----|
| AmazonEKSFargateServiceRolePolicy | 392 |
| Uso de esta política | 392 |
| Detalles de la política | 392 |
| Versión de la política | 392 |
| Documento de política JSON | 392 |
| Más información | 393 |
| AmazonEKSLocalOutpostClusterPolicy | 393 |
| Uso de esta política | 393 |
| Detalles de la política | 393 |
| Versión de la política | 393 |
| Documento de política JSON | 394 |
| Más información | 395 |
| AmazonEKSLocalOutpostServiceRolePolicy | 396 |
| Uso de esta política | 396 |
| Detalles de la política | 396 |
| Versión de la política | 396 |
| Documento de política JSON | 396 |
| Más información | 402 |
| AmazonEKSServicePolicy | 402 |
| Uso de esta política | 402 |
| Detalles de la política | 402 |
| Versión de la política | 403 |
| Documento de política JSON | 403 |
| Más información | 404 |
| AmazonEKSServiceRolePolicy | 405 |
| Uso de esta política | 405 |
| Detalles de la política | 405 |
| Versión de la política | 405 |
| Documento de política JSON | 405 |
| Más información | 408 |
| AmazonEKSVPCResourceController | 408 |
| Uso de esta política | 408 |
| Detalles de la política | 408 |
| Versión de la política | 408 |
| Documento de política JSON | 408 |
| Más información | 409 |

| | |
|---|-----|
| AmazonEKSElasticContainerRegistryPublicFullAccess | 409 |
| Uso de esta política | 409 |
| Información de la política | 410 |
| Versión de la política | 410 |
| Documento de política JSON | 410 |
| Más información | 411 |
| AmazonElasticContainerRegistryPublicPowerUser | 411 |
| Uso de la política | 411 |
| Información de la política | 411 |
| Versión de la política | 411 |
| Documento de política JSON | 411 |
| Más información | 415 |
| AmazonElasticContainerRegistryPublicReadOnly | 415 |
| Uso de esta política | 415 |
| Detalles de la política | 415 |
| Versión de la política | 415 |
| Documento de política JSON | 416 |
| Más información | 416 |
| AmazonElasticContainerRegistryPublicFullAccess | 416 |
| Uso de esta política | 416 |
| Detalles de la política | 416 |
| Versión de la política | 417 |
| Documento de política JSON | 417 |
| Más información | 417 |
| AmazonElasticContainerRegistryPublicPowerUser | 418 |
| Uso de esta política | 418 |
| Detalles de la política | 418 |
| Versión de la política | 418 |
| Documento de política JSON | 418 |
| Más información | 419 |
| AmazonElasticContainerRegistryPublicReadOnly | 419 |
| Uso de esta política | 419 |
| Detalles de la política | 419 |
| Versión de la política | 420 |
| Documento de política JSON | 420 |
| Más información | 420 |

| | |
|--|-----|
| AmazonElasticFileSystemClientFullAccess | 421 |
| Uso de esta política | 421 |
| Detalles de la política | 421 |
| Versión de la política | 421 |
| Documento de política JSON | 421 |
| Más información | 422 |
| AmazonElasticFileSystemClientReadOnlyAccess | 422 |
| Uso de esta política | 422 |
| Detalles de la política | 422 |
| Versión de la política | 422 |
| Documento de política JSON | 423 |
| Más información | 423 |
| AmazonElasticFileSystemClientReadWriteAccess | 423 |
| Uso de esta política | 423 |
| Detalles de la política | 424 |
| Versión de la política | 424 |
| Documento de política JSON | 424 |
| Más información | 424 |
| AmazonElasticFileSystemFullAccess | 425 |
| Uso de esta política | 425 |
| Información de la política | 425 |
| Versión de la política | 425 |
| Documento de política JSON | 425 |
| Más información | 427 |
| AmazonElasticFileSystemReadOnlyAccess | 427 |
| Uso de esta política | 427 |
| Detalles de la política | 427 |
| Versión de la política | 428 |
| Documento de política JSON | 428 |
| Más información | 429 |
| AmazonElasticFileSystemServiceRolePolicy | 429 |
| Uso de esta política | 429 |
| Detalles de la política | 429 |
| Versión de la política | 429 |
| Documento de política JSON | 430 |
| Más información | 432 |

| | |
|--|-----|
| AmazonElasticFileSystemsUtils | 432 |
| Uso de esta política | 432 |
| Detalles de la política | 432 |
| Versión de la política | 432 |
| Documento de política JSON | 433 |
| Más información | 434 |
| AmazonElasticMapReduceEditorsRole | 435 |
| Uso de esta política | 435 |
| Detalles de la política | 435 |
| Versión de la política | 435 |
| Documento de política JSON | 435 |
| Más información | 436 |
| AmazonElasticMapReduceforAutoScalingRole | 437 |
| Uso de esta política | 437 |
| Detalles de la política | 437 |
| Versión de la política | 437 |
| Documento de política JSON | 437 |
| Más información | 438 |
| AmazonElasticMapReduceforEC2Role | 438 |
| Uso de esta política | 438 |
| Detalles de la política | 438 |
| Versión de la política | 438 |
| Documento de política JSON | 439 |
| Más información | 440 |
| AmazonElasticMapReduceFullAccess | 440 |
| Uso de esta política | 441 |
| Detalles de la política | 441 |
| Versión de la política | 441 |
| Documento de política JSON | 441 |
| Más información | 443 |
| AmazonElasticMapReducePlacementGroupPolicy | 443 |
| Uso de esta política | 443 |
| Detalles de la política | 443 |
| Versión de la política | 443 |
| Documento de política JSON | 444 |
| Más información | 444 |

| | |
|--|-----|
| AmazonElasticMapReduceReadOnlyAccess | 444 |
| Uso de esta política | 445 |
| Detalles de la política | 445 |
| Versión de la política | 445 |
| Documento de política JSON | 445 |
| Más información | 446 |
| AmazonElasticMapReduceRole | 446 |
| Uso de esta política | 446 |
| Detalles de la política | 446 |
| Versión de la política | 446 |
| Documento de política JSON | 447 |
| Más información | 449 |
| AmazonElasticsearchServiceRolePolicy | 449 |
| Uso de esta política | 449 |
| Detalles de la política | 449 |
| Versión de la política | 449 |
| Documento de política JSON | 450 |
| Más información | 452 |
| AmazonElasticTranscoder_FullAccess | 453 |
| Uso de esta política | 453 |
| Detalles de la política | 453 |
| Versión de la política | 453 |
| Documento de política JSON | 453 |
| Más información | 454 |
| AmazonElasticTranscoder_JobsSubmitter | 454 |
| Uso de esta política | 454 |
| Detalles de la política | 455 |
| Versión de la política | 455 |
| Documento de política JSON | 455 |
| Más información | 456 |
| AmazonElasticTranscoder_ReadOnlyAccess | 456 |
| Uso de esta política | 456 |
| Detalles de la política | 456 |
| Versión de la política | 456 |
| Documento de política JSON | 456 |
| Más información | 457 |

| | |
|--|-----|
| AmazonElasticTranscoderRole | 457 |
| Uso de esta política | 457 |
| Detalles de la política | 457 |
| Versión de la política | 458 |
| Documento de política JSON | 458 |
| Más información | 459 |
| AmazonEMRCleanupPolicy | 459 |
| Uso de esta política | 459 |
| Detalles de la política | 459 |
| Versión de la política | 459 |
| Documento de política JSON | 460 |
| Más información | 460 |
| AmazonEMRContainersServiceRolePolicy | 460 |
| Uso de esta política | 461 |
| Detalles de la política | 461 |
| Versión de la política | 461 |
| Documento de política JSON | 461 |
| Más información | 462 |
| AmazonEMRFullAccessPolicy_v2 | 462 |
| Uso de esta política | 463 |
| Detalles de la política | 463 |
| Versión de la política | 463 |
| Documento de política JSON | 463 |
| Más información | 466 |
| AmazonEMRReadOnlyAccessPolicy_v2 | 467 |
| Uso de esta política | 467 |
| Detalles de la política | 467 |
| Versión de la política | 467 |
| Documento de política JSON | 467 |
| Más información | 468 |
| AmazonEMRServerlessServiceRolePolicy | 469 |
| Uso de esta política | 469 |
| Información de la política | 469 |
| Versión de la política | 469 |
| Documento de política JSON | 469 |
| Más información | 470 |

| | |
|---|-----|
| AmazonEMRServicePolicy_v2 | 470 |
| Uso de esta política | 471 |
| Detalles de la política | 471 |
| Versión de la política | 471 |
| Documento de política JSON | 471 |
| Más información | 479 |
| AmazonESCognitoAccess | 479 |
| Uso de esta política | 479 |
| Detalles de la política | 479 |
| Versión de la política | 479 |
| Documento de política JSON | 479 |
| Más información | 480 |
| AmazonESFullAccess | 481 |
| Uso de esta política | 481 |
| Detalles de la política | 481 |
| Versión de la política | 481 |
| Documento de política JSON | 481 |
| Más información | 482 |
| AmazonESReadOnlyAccess | 482 |
| Uso de esta política | 482 |
| Detalles de la política | 482 |
| Versión de la política | 482 |
| Documento de política JSON | 483 |
| Más información | 483 |
| AmazonEventBridgeApiDestinationsServiceRolePolicy | 483 |
| Uso de esta política | 483 |
| Detalles de la política | 483 |
| Versión de la política | 484 |
| Documento de política JSON | 484 |
| Más información | 484 |
| AmazonEventBridgeFullAccess | 485 |
| Uso de esta política | 485 |
| Detalles de la política | 485 |
| Versión de la política | 485 |
| Documento de política JSON | 485 |
| Más información | 487 |

| | |
|--|-----|
| AmazonEventBridgePipesFullAccess | 488 |
| Uso de esta política | 488 |
| Detalles de la política | 488 |
| Versión de la política | 488 |
| Documento de política JSON | 488 |
| Más información | 489 |
| AmazonEventBridgePipesOperatorAccess | 489 |
| Uso de esta política | 489 |
| Detalles de la política | 489 |
| Versión de la política | 490 |
| Documento de política JSON | 490 |
| Más información | 490 |
| AmazonEventBridgePipesReadOnlyAccess | 491 |
| Uso de esta política | 491 |
| Detalles de la política | 491 |
| Versión de la política | 491 |
| Documento de política JSON | 491 |
| Más información | 492 |
| AmazonEventBridgeReadOnlyAccess | 492 |
| Uso de esta política | 492 |
| Detalles de la política | 492 |
| Versión de la política | 492 |
| Documento de política JSON | 493 |
| Más información | 494 |
| AmazonEventBridgeSchedulerFullAccess | 494 |
| Uso de esta política | 494 |
| Detalles de la política | 494 |
| Versión de la política | 495 |
| Documento de política JSON | 495 |
| Más información | 495 |
| AmazonEventBridgeSchedulerReadOnlyAccess | 496 |
| Uso de esta política | 496 |
| Detalles de la política | 496 |
| Versión de la política | 496 |
| Documento de política JSON | 496 |
| Más información | 497 |

| | |
|---|-----|
| AmazonEventBridgeSchemasFullAccess | 497 |
| Uso de esta política | 497 |
| Detalles de la política | 497 |
| Versión de la política | 497 |
| Documento de política JSON | 498 |
| Más información | 498 |
| AmazonEventBridgeSchemasReadOnlyAccess | 499 |
| Uso de esta política | 499 |
| Detalles de la política | 499 |
| Versión de la política | 499 |
| Documento de política JSON | 499 |
| Más información | 500 |
| AmazonEventBridgeSchemasServiceRolePolicy | 500 |
| Uso de esta política | 500 |
| Detalles de la política | 501 |
| Versión de la política | 501 |
| Documento de política JSON | 501 |
| Más información | 502 |
| AmazonFISServiceRolePolicy | 502 |
| Uso de esta política | 502 |
| Detalles de la política | 502 |
| Versión de la política | 502 |
| Documento de política JSON | 502 |
| Más información | 504 |
| AmazonForecastFullAccess | 504 |
| Uso de esta política | 504 |
| Detalles de la política | 504 |
| Versión de la política | 505 |
| Documento de política JSON | 505 |
| Más información | 505 |
| AmazonFraudDetectorFullAccessPolicy | 506 |
| Uso de esta política | 506 |
| Detalles de la política | 506 |
| Versión de la política | 506 |
| Documento de política JSON | 506 |
| Más información | 507 |

| | |
|--------------------------------------|-----|
| AmazonFreeRTOSFullAccess | 508 |
| Uso de esta política | 508 |
| Detalles de la política | 508 |
| Versión de la política | 508 |
| Documento de política JSON | 508 |
| Más información | 509 |
| AmazonFreeRTOSOTAUpdate | 509 |
| Uso de esta política | 509 |
| Detalles de la política | 509 |
| Versión de la política | 509 |
| Documento de política JSON | 510 |
| Más información | 511 |
| AmazonFSxConsoleFullAccess | 511 |
| Uso de esta política | 511 |
| Información de la política | 512 |
| Versión de la política | 512 |
| Documento de política JSON | 512 |
| Más información | 515 |
| AmazonFSxConsoleReadOnlyAccess | 516 |
| Uso de esta política | 516 |
| Información de la política | 516 |
| Versión de la política | 516 |
| Documento de política JSON | 516 |
| Más información | 517 |
| AmazonFSxFullAccess | 517 |
| Uso de esta política | 517 |
| Información de la política | 517 |
| Versión de la política | 518 |
| Documento de política JSON | 518 |
| Más información | 522 |
| AmazonFSxReadOnlyAccess | 522 |
| Uso de esta política | 522 |
| Detalles de la política | 522 |
| Versión de la política | 522 |
| Documento de política JSON | 523 |
| Más información | 523 |

| | |
|-------------------------------------|-----|
| AmazonFSxServiceRolePolicy | 523 |
| Uso de esta política | 523 |
| Información de la política | 524 |
| Versión de la política | 524 |
| Documento de política JSON | 524 |
| Más información | 527 |
| AmazonGlacierFullAccess | 527 |
| Uso de esta política | 527 |
| Detalles de la política | 527 |
| Versión de la política | 527 |
| Documento de política JSON | 527 |
| Más información | 528 |
| AmazonGlacierReadOnlyAccess | 528 |
| Uso de esta política | 528 |
| Detalles de la política | 528 |
| Versión de la política | 529 |
| Documento de política JSON | 529 |
| Más información | 529 |
| AmazonGrafanaAthenaAccess | 530 |
| Uso de esta política | 530 |
| Detalles de la política | 530 |
| Versión de la política | 530 |
| Documento de política JSON | 530 |
| Más información | 532 |
| AmazonGrafanaCloudWatchAccess | 532 |
| Uso de esta política | 532 |
| Detalles de la política | 533 |
| Versión de la política | 533 |
| Documento de política JSON | 533 |
| Más información | 534 |
| AmazonGrafanaRedshiftAccess | 535 |
| Uso de esta política | 535 |
| Detalles de la política | 535 |
| Versión de la política | 535 |
| Documento de política JSON | 535 |
| Más información | 536 |

| | |
|---|-----|
| AmazonGrafanaServiceLinkedRolePolicy | 537 |
| Uso de esta política | 537 |
| Detalles de la política | 537 |
| Versión de la política | 537 |
| Documento de política JSON | 537 |
| Más información | 539 |
| AmazonGuardDutyFullAccess | 539 |
| Uso de la política | 539 |
| Información de la política | 539 |
| Versión de la política | 539 |
| Documento de política JSON | 539 |
| Más información | 541 |
| AmazonGuardDutyMalwareProtectionServiceRolePolicy | 541 |
| Uso de la política | 541 |
| Información de la política | 541 |
| Versión de la política | 542 |
| Documento de política JSON | 542 |
| Más información | 546 |
| AmazonGuardDutyReadOnlyAccess | 546 |
| Uso de la política | 546 |
| Información de la política | 547 |
| Versión de la política | 547 |
| Documento de política JSON | 547 |
| Más información | 548 |
| AmazonGuardDutyServiceRolePolicy | 548 |
| Uso de la política | 548 |
| Información de la política | 548 |
| Versión de la política | 548 |
| Documento de política JSON | 549 |
| Más información | 553 |
| AmazonHealthLakeFullAccess | 553 |
| Uso de esta política | 554 |
| Detalles de la política | 554 |
| Versión de la política | 554 |
| Documento de política JSON | 554 |
| Más información | 555 |

| | |
|--|-----|
| AmazonHealthLakeReadOnlyAccess | 555 |
| Uso de esta política | 555 |
| Detalles de la política | 555 |
| Versión de la política | 555 |
| Documento de política JSON | 556 |
| Más información | 556 |
| AmazonHoneycodeFullAccess | 556 |
| Uso de esta política | 557 |
| Detalles de la política | 557 |
| Versión de la política | 557 |
| Documento de política JSON | 557 |
| Más información | 557 |
| AmazonHoneycodeReadOnlyAccess | 558 |
| Uso de esta política | 558 |
| Detalles de la política | 558 |
| Versión de la política | 558 |
| Documento de política JSON | 558 |
| Más información | 559 |
| AmazonHoneycodeServiceRolePolicy | 559 |
| Uso de esta política | 559 |
| Detalles de la política | 559 |
| Versión de la política | 560 |
| Documento de política JSON | 560 |
| Más información | 560 |
| AmazonHoneycodeTeamAssociationFullAccess | 560 |
| Uso de esta política | 560 |
| Detalles de la política | 561 |
| Versión de la política | 561 |
| Documento de política JSON | 561 |
| Más información | 561 |
| AmazonHoneycodeTeamAssociationReadOnlyAccess | 562 |
| Uso de esta política | 562 |
| Detalles de la política | 562 |
| Versión de la política | 562 |
| Documento de política JSON | 562 |
| Más información | 563 |

| | |
|--|-----|
| AmazonHoneycodeWorkbookFullAccess | 563 |
| Uso de esta política | 563 |
| Detalles de la política | 563 |
| Versión de la política | 563 |
| Documento de política JSON | 564 |
| Más información | 564 |
| AmazonHoneycodeWorkbookReadOnlyAccess | 565 |
| Uso de esta política | 565 |
| Detalles de la política | 565 |
| Versión de la política | 565 |
| Documento de política JSON | 565 |
| Más información | 566 |
| AmazonInspector2AgentlessServiceRolePolicy | 566 |
| Uso de la política | 566 |
| Información de la política | 566 |
| Versión de la política | 566 |
| Documento de política JSON | 567 |
| Más información | 570 |
| AmazonInspector2FullAccess | 570 |
| Uso de esta política | 571 |
| Detalles de la política | 571 |
| Versión de la política | 571 |
| Documento de política JSON | 571 |
| Más información | 572 |
| AmazonInspector2ManagedCisPolicy | 572 |
| Uso de la política | 573 |
| Información de la política | 573 |
| Versión de la política | 573 |
| Documento de política JSON | 573 |
| Más información | 574 |
| AmazonInspector2ReadOnlyAccess | 574 |
| Uso de esta política | 574 |
| Detalles de la política | 574 |
| Versión de la política | 574 |
| Documento de política JSON | 574 |
| Más información | 575 |

| | |
|---|-----|
| AmazonInspector2ServiceRolePolicy | 575 |
| Uso de esta política | 575 |
| Información de la política | 576 |
| Versión de la política | 576 |
| Documento de política JSON | 576 |
| Más información | 582 |
| AmazonInspectorFullAccess | 583 |
| Uso de esta política | 583 |
| Detalles de la política | 583 |
| Versión de la política | 583 |
| Documento de política JSON | 583 |
| Más información | 584 |
| AmazonInspectorReadOnlyAccess | 585 |
| Uso de esta política | 585 |
| Detalles de la política | 585 |
| Versión de la política | 585 |
| Documento de política JSON | 585 |
| Más información | 586 |
| AmazonInspectorServiceRolePolicy | 586 |
| Uso de esta política | 586 |
| Detalles de la política | 586 |
| Versión de la política | 586 |
| Documento de política JSON | 587 |
| Más información | 588 |
| AmazonKendraFullAccess | 588 |
| Uso de esta política | 588 |
| Detalles de la política | 588 |
| Versión de la política | 589 |
| Documento de política JSON | 589 |
| Más información | 591 |
| AmazonKendraReadOnlyAccess | 591 |
| Uso de esta política | 591 |
| Detalles de la política | 591 |
| Versión de la política | 591 |
| Documento de política JSON | 591 |
| Más información | 592 |

| | |
|--|-----|
| AmazonKeyspacesFullAccess | 592 |
| Uso de esta política | 592 |
| Detalles de la política | 592 |
| Versión de la política | 593 |
| Documento de política JSON | 593 |
| Más información | 595 |
| AmazonKeyspacesReadOnlyAccess | 595 |
| Uso de esta política | 595 |
| Detalles de la política | 595 |
| Versión de la política | 595 |
| Documento de política JSON | 595 |
| Más información | 596 |
| AmazonKeyspacesReadOnlyAccess_v2 | 596 |
| Uso de esta política | 597 |
| Detalles de la política | 597 |
| Versión de la política | 597 |
| Documento de política JSON | 597 |
| Más información | 598 |
| AmazonKinesisAnalyticsFullAccess | 598 |
| Uso de esta política | 598 |
| Detalles de la política | 598 |
| Versión de la política | 599 |
| Documento de política JSON | 599 |
| Más información | 600 |
| AmazonKinesisAnalyticsReadOnly | 600 |
| Uso de esta política | 601 |
| Detalles de la política | 601 |
| Versión de la política | 601 |
| Documento de política JSON | 601 |
| Más información | 602 |
| AmazonKinesisFirehoseFullAccess | 603 |
| Uso de esta política | 603 |
| Detalles de la política | 603 |
| Versión de la política | 603 |
| Documento de política JSON | 603 |
| Más información | 604 |

| | |
|---|-----|
| AmazonKinesisFirehoseReadOnlyAccess | 604 |
| Uso de esta política | 604 |
| Detalles de la política | 604 |
| Versión de la política | 604 |
| Documento de política JSON | 604 |
| Más información | 605 |
| AmazonKinesisFullAccess | 605 |
| Uso de esta política | 605 |
| Detalles de la política | 605 |
| Versión de la política | 606 |
| Documento de política JSON | 606 |
| Más información | 606 |
| AmazonKinesisReadOnlyAccess | 606 |
| Uso de esta política | 606 |
| Detalles de la política | 607 |
| Versión de la política | 607 |
| Documento de política JSON | 607 |
| Más información | 607 |
| AmazonKinesisVideoStreamsFullAccess | 608 |
| Uso de esta política | 608 |
| Detalles de la política | 608 |
| Versión de la política | 608 |
| Documento de política JSON | 608 |
| Más información | 609 |
| AmazonKinesisVideoStreamsReadOnlyAccess | 609 |
| Uso de esta política | 609 |
| Detalles de la política | 609 |
| Versión de la política | 609 |
| Documento de política JSON | 610 |
| Más información | 610 |
| AmazonLaunchWizard_Fullaccess | 610 |
| Uso de esta política | 610 |
| Detalles de la política | 610 |
| Versión de la política | 611 |
| Documento de política JSON | 611 |
| Más información | 625 |

| | |
|--------------------------------------|-----|
| AmazonLaunchWizardFullAccessV2 | 625 |
| Uso de esta política | 625 |
| Detalles de la política | 625 |
| Versión de la política | 626 |
| Documento de política JSON | 626 |
| Más información | 642 |
| AmazonLexChannelsAccess | 643 |
| Uso de esta política | 643 |
| Detalles de la política | 643 |
| Versión de la política | 643 |
| Documento de política JSON | 643 |
| Más información | 644 |
| AmazonLexFullAccess | 644 |
| Uso de esta política | 644 |
| Información de la política | 644 |
| Versión de la política | 644 |
| Documento de política JSON | 645 |
| Más información | 650 |
| AmazonLexReadOnly | 650 |
| Uso de esta política | 650 |
| Detalles de la política | 650 |
| Versión de la política | 651 |
| Documento de política JSON | 651 |
| Más información | 652 |
| AmazonLexReplicationPolicy | 653 |
| Uso de la política | 653 |
| Información de la política | 653 |
| Versión de la política | 653 |
| Documento de política JSON | 653 |
| Más información | 655 |
| AmazonLexRunBotsOnly | 656 |
| Uso de esta política | 656 |
| Detalles de la política | 656 |
| Versión de la política | 656 |
| Documento de política JSON | 656 |
| Más información | 657 |

| | |
|--|-----|
| AmazonLexV2BotPolicy | 657 |
| Uso de esta política | 657 |
| Detalles de la política | 657 |
| Versión de la política | 657 |
| Documento de política JSON | 658 |
| Más información | 658 |
| AmazonLookoutEquipmentFullAccess | 658 |
| Uso de esta política | 658 |
| Detalles de la política | 658 |
| Versión de la política | 659 |
| Documento de política JSON | 659 |
| Más información | 660 |
| AmazonLookoutEquipmentReadOnlyAccess | 660 |
| Uso de esta política | 660 |
| Detalles de la política | 661 |
| Versión de la política | 661 |
| Documento de política JSON | 661 |
| Más información | 661 |
| AmazonLookoutMetricsFullAccess | 662 |
| Uso de esta política | 662 |
| Detalles de la política | 662 |
| Versión de la política | 662 |
| Documento de política JSON | 662 |
| Más información | 663 |
| AmazonLookoutMetricsReadOnlyAccess | 663 |
| Uso de esta política | 663 |
| Detalles de la política | 663 |
| Versión de la política | 664 |
| Documento de política JSON | 664 |
| Más información | 665 |
| AmazonLookoutVisionConsoleFullAccess | 665 |
| Uso de esta política | 665 |
| Detalles de la política | 665 |
| Versión de la política | 665 |
| Documento de política JSON | 665 |
| Más información | 668 |

| | |
|---|-----|
| AmazonLookoutVisionConsoleReadOnlyAccess | 668 |
| Uso de esta política | 668 |
| Detalles de la política | 668 |
| Versión de la política | 668 |
| Documento de política JSON | 669 |
| Más información | 670 |
| AmazonLookoutVisionFullAccess | 670 |
| Uso de esta política | 670 |
| Detalles de la política | 670 |
| Versión de la política | 670 |
| Documento de política JSON | 671 |
| Más información | 671 |
| AmazonLookoutVisionReadOnlyAccess | 671 |
| Uso de esta política | 671 |
| Detalles de la política | 672 |
| Versión de la política | 672 |
| Documento de política JSON | 672 |
| Más información | 673 |
| AmazonMachineLearningBatchPredictionsAccess | 673 |
| Uso de esta política | 673 |
| Detalles de la política | 673 |
| Versión de la política | 673 |
| Documento de política JSON | 674 |
| Más información | 674 |
| AmazonMachineLearningCreateOnlyAccess | 674 |
| Uso de esta política | 674 |
| Detalles de la política | 675 |
| Versión de la política | 675 |
| Documento de política JSON | 675 |
| Más información | 675 |
| AmazonMachineLearningFullAccess | 676 |
| Uso de esta política | 676 |
| Detalles de la política | 676 |
| Versión de la política | 676 |
| Documento de política JSON | 676 |
| Más información | 677 |

| | |
|---|-----|
| AmazonMachineLearningManageRealTimeEndpointOnlyAccess | 677 |
| Uso de esta política | 677 |
| Detalles de la política | 677 |
| Versión de la política | 677 |
| Documento de política JSON | 678 |
| Más información | 678 |
| AmazonMachineLearningReadOnlyAccess | 678 |
| Uso de esta política | 678 |
| Detalles de la política | 679 |
| Versión de la política | 679 |
| Documento de política JSON | 679 |
| Más información | 679 |
| AmazonMachineLearningRealTimePredictionOnlyAccess | 680 |
| Uso de esta política | 680 |
| Detalles de la política | 680 |
| Versión de la política | 680 |
| Documento de política JSON | 680 |
| Más información | 681 |
| AmazonMachineLearningRoleforRedshiftDataSourceV3 | 681 |
| Uso de esta política | 681 |
| Detalles de la política | 681 |
| Versión de la política | 682 |
| Documento de política JSON | 682 |
| Más información | 683 |
| AmazonMacieFullAccess | 683 |
| Uso de esta política | 683 |
| Detalles de la política | 683 |
| Versión de la política | 683 |
| Documento de política JSON | 684 |
| Más información | 684 |
| AmazonMacieHandshakeRole | 685 |
| Uso de esta política | 685 |
| Detalles de la política | 685 |
| Versión de la política | 685 |
| Documento de política JSON | 685 |
| Más información | 686 |

| | |
|--|-----|
| AmazonMacieReadOnlyAccess | 686 |
| Uso de esta política | 686 |
| Detalles de la política | 686 |
| Versión de la política | 686 |
| Documento de política JSON | 687 |
| Más información | 687 |
| AmazonMacieServiceRole | 687 |
| Uso de esta política | 687 |
| Detalles de la política | 688 |
| Versión de la política | 688 |
| Documento de política JSON | 688 |
| Más información | 688 |
| AmazonMacieServiceRolePolicy | 689 |
| Uso de esta política | 689 |
| Detalles de la política | 689 |
| Versión de la política | 689 |
| Documento de política JSON | 689 |
| Más información | 691 |
| AmazonManagedBlockchainConsoleFullAccess | 691 |
| Uso de esta política | 691 |
| Detalles de la política | 691 |
| Versión de la política | 691 |
| Documento de política JSON | 691 |
| Más información | 692 |
| AmazonManagedBlockchainFullAccess | 692 |
| Uso de esta política | 692 |
| Detalles de la política | 692 |
| Versión de la política | 693 |
| Documento de política JSON | 693 |
| Más información | 693 |
| AmazonManagedBlockchainReadOnlyAccess | 694 |
| Uso de esta política | 694 |
| Detalles de la política | 694 |
| Versión de la política | 694 |
| Documento de política JSON | 694 |
| Más información | 695 |

| | |
|--|-----|
| AmazonManagedBlockchainServiceRolePolicy | 695 |
| Uso de esta política | 695 |
| Detalles de la política | 695 |
| Versión de la política | 695 |
| Documento de política JSON | 696 |
| Más información | 696 |
| AmazonMCSFullAccess | 696 |
| Uso de esta política | 697 |
| Detalles de la política | 697 |
| Versión de la política | 697 |
| Documento de política JSON | 697 |
| Más información | 698 |
| AmazonMCSReadOnlyAccess | 699 |
| Uso de esta política | 699 |
| Detalles de la política | 699 |
| Versión de la política | 699 |
| Documento de política JSON | 699 |
| Más información | 700 |
| AmazonMechanicalTurkFullAccess | 700 |
| Uso de esta política | 700 |
| Detalles de la política | 700 |
| Versión de la política | 701 |
| Documento de política JSON | 701 |
| Más información | 701 |
| AmazonMechanicalTurkReadOnly | 701 |
| Uso de esta política | 702 |
| Detalles de la política | 702 |
| Versión de la política | 702 |
| Documento de política JSON | 702 |
| Más información | 703 |
| AmazonMemoryDBFullAccess | 703 |
| Uso de esta política | 703 |
| Detalles de la política | 703 |
| Versión de la política | 703 |
| Documento de política JSON | 703 |
| Más información | 704 |

| | |
|--|-----|
| AmazonMemoryDBReadOnlyAccess | 704 |
| Uso de esta política | 704 |
| Detalles de la política | 705 |
| Versión de la política | 705 |
| Documento de política JSON | 705 |
| Más información | 705 |
| AmazonMobileAnalyticsFinancialReportAccess | 706 |
| Uso de esta política | 706 |
| Detalles de la política | 706 |
| Versión de la política | 706 |
| Documento de política JSON | 706 |
| Más información | 707 |
| AmazonMobileAnalyticsFullAccess | 707 |
| Uso de esta política | 707 |
| Detalles de la política | 707 |
| Versión de la política | 707 |
| Documento de política JSON | 708 |
| Más información | 708 |
| AmazonMobileAnalyticsNon-financialReportAccess | 708 |
| Uso de esta política | 708 |
| Detalles de la política | 709 |
| Versión de la política | 709 |
| Documento de política JSON | 709 |
| Más información | 709 |
| AmazonMobileAnalyticsWriteOnlyAccess | 710 |
| Uso de esta política | 710 |
| Detalles de la política | 710 |
| Versión de la política | 710 |
| Documento de política JSON | 710 |
| Más información | 711 |
| AmazonMonitronFullAccess | 711 |
| Uso de esta política | 711 |
| Detalles de la política | 711 |
| Versión de la política | 711 |
| Documento de política JSON | 711 |
| Más información | 713 |

| | |
|--------------------------------------|-----|
| AmazonMQApiFullAccess | 714 |
| Uso de esta política | 714 |
| Detalles de la política | 714 |
| Versión de la política | 714 |
| Documento de política JSON | 714 |
| Más información | 715 |
| AmazonMQApiReadOnlyAccess | 716 |
| Uso de esta política | 716 |
| Detalles de la política | 716 |
| Versión de la política | 716 |
| Documento de política JSON | 716 |
| Más información | 717 |
| AmazonMQFullAccess | 717 |
| Uso de esta política | 717 |
| Detalles de la política | 717 |
| Versión de la política | 717 |
| Documento de política JSON | 718 |
| Más información | 719 |
| AmazonMQReadOnlyAccess | 719 |
| Uso de esta política | 719 |
| Detalles de la política | 719 |
| Versión de la política | 719 |
| Documento de política JSON | 720 |
| Más información | 720 |
| AmazonMQServiceRolePolicy | 720 |
| Uso de esta política | 721 |
| Detalles de la política | 721 |
| Versión de la política | 721 |
| Documento de política JSON | 721 |
| Más información | 723 |
| AmazonMSKConnectReadOnlyAccess | 723 |
| Uso de esta política | 723 |
| Detalles de la política | 723 |
| Versión de la política | 723 |
| Documento de política JSON | 724 |
| Más información | 725 |

| | |
|--|-----|
| AmazonMSKFullAccess | 725 |
| Uso de esta política | 725 |
| Detalles de la política | 725 |
| Versión de la política | 725 |
| Documento de política JSON | 726 |
| Más información | 728 |
| AmazonMSKReadOnlyAccess | 729 |
| Uso de esta política | 729 |
| Detalles de la política | 729 |
| Versión de la política | 729 |
| Documento de política JSON | 729 |
| Más información | 730 |
| AmazonMWAAServiceRolePolicy | 730 |
| Uso de esta política | 730 |
| Detalles de la política | 730 |
| Versión de la política | 730 |
| Documento de política JSON | 731 |
| Más información | 733 |
| AmazonNimbleStudio-LaunchProfileWorker | 733 |
| Uso de esta política | 733 |
| Detalles de la política | 733 |
| Versión de la política | 733 |
| Documento de política JSON | 734 |
| Más información | 734 |
| AmazonNimbleStudio-StudioAdmin | 735 |
| Uso de esta política | 735 |
| Detalles de la política | 735 |
| Versión de la política | 735 |
| Documento de política JSON | 735 |
| Más información | 737 |
| AmazonNimbleStudio-StudioUser | 737 |
| Uso de esta política | 737 |
| Detalles de la política | 738 |
| Versión de la política | 738 |
| Documento de política JSON | 738 |
| Más información | 740 |

| | |
|---|-----|
| AmazonOmicsFullAccess | 740 |
| Uso de esta política | 740 |
| Detalles de la política | 741 |
| Versión de la política | 741 |
| Documento de política JSON | 741 |
| Más información | 742 |
| AmazonOmicsReadOnlyAccess | 742 |
| Uso de esta política | 742 |
| Detalles de la política | 742 |
| Versión de la política | 743 |
| Documento de política JSON | 743 |
| Más información | 743 |
| AmazonOneEnterpriseFullAccess | 743 |
| Uso de la política | 744 |
| Información de la política | 744 |
| Versión de la política | 744 |
| Documento de política JSON | 744 |
| Más información | 744 |
| AmazonOneEnterpriseInstallerAccess | 745 |
| Uso de la política | 745 |
| Información de la política | 745 |
| Versión de la política | 745 |
| Documento de política JSON | 745 |
| Más información | 746 |
| AmazonOneEnterpriseReadOnlyAccess | 746 |
| Uso de la política | 746 |
| Información de la política | 746 |
| Versión de la política | 747 |
| Documento de política JSON | 747 |
| Más información | 747 |
| AmazonOpenSearchDashboardsServiceRolePolicy | 747 |
| Uso de la política | 748 |
| Información de la política | 748 |
| Versión de la política | 748 |
| Documento de política JSON | 748 |
| Más información | 749 |

| | |
|---|-----|
| AmazonOpenSearchIngestionFullAccess | 749 |
| Uso de esta política | 749 |
| Detalles de la política | 749 |
| Versión de la política | 749 |
| Documento de política JSON | 749 |
| Más información | 750 |
| AmazonOpenSearchIngestionReadOnlyAccess | 751 |
| Uso de esta política | 751 |
| Detalles de la política | 751 |
| Versión de la política | 751 |
| Documento de política JSON | 751 |
| Más información | 752 |
| AmazonOpenSearchIngestionServiceRolePolicy | 752 |
| Uso de esta política | 752 |
| Detalles de la política | 752 |
| Versión de la política | 753 |
| Documento de política JSON | 753 |
| Más información | 755 |
| AmazonOpenSearchServerlessServiceRolePolicy | 755 |
| Uso de esta política | 755 |
| Detalles de la política | 755 |
| Versión de la política | 755 |
| Documento de política JSON | 755 |
| Más información | 756 |
| AmazonOpenSearchServiceCognitoAccess | 756 |
| Uso de esta política | 756 |
| Detalles de la política | 756 |
| Versión de la política | 757 |
| Documento de política JSON | 757 |
| Más información | 758 |
| AmazonOpenSearchServiceFullAccess | 758 |
| Uso de esta política | 758 |
| Detalles de la política | 758 |
| Versión de la política | 759 |
| Documento de política JSON | 759 |
| Más información | 759 |

| | |
|---|-----|
| AmazonOpenSearchServiceReadOnlyAccess | 759 |
| Uso de esta política | 760 |
| Detalles de la política | 760 |
| Versión de la política | 760 |
| Documento de política JSON | 760 |
| Más información | 761 |
| AmazonOpenSearchServiceRolePolicy | 761 |
| Uso de esta política | 761 |
| Detalles de la política | 761 |
| Versión de la política | 761 |
| Documento de política JSON | 762 |
| Más información | 766 |
| AmazonPersonalizeFullAccess | 766 |
| Uso de esta política | 766 |
| Detalles de la política | 767 |
| Versión de la política | 767 |
| Documento de política JSON | 767 |
| Más información | 768 |
| AmazonPollyFullAccess | 768 |
| Uso de esta política | 768 |
| Detalles de la política | 769 |
| Versión de la política | 769 |
| Documento de política JSON | 769 |
| Más información | 769 |
| AmazonPollyReadOnlyAccess | 770 |
| Uso de esta política | 770 |
| Detalles de la política | 770 |
| Versión de la política | 770 |
| Documento de política JSON | 770 |
| Más información | 771 |
| AmazonPrometheusConsoleFullAccess | 771 |
| Uso de esta política | 771 |
| Detalles de la política | 771 |
| Versión de la política | 772 |
| Documento de política JSON | 772 |
| Más información | 773 |

| | |
|---|-----|
| AmazonPrometheusFullAccess | 773 |
| Uso de esta política | 773 |
| Información de la política | 773 |
| Versión de la política | 773 |
| Documento de política JSON | 774 |
| Más información | 775 |
| AmazonPrometheusQueryAccess | 775 |
| Uso de esta política | 775 |
| Detalles de la política | 775 |
| Versión de la política | 775 |
| Documento de política JSON | 776 |
| Más información | 776 |
| AmazonPrometheusRemoteWriteAccess | 776 |
| Uso de esta política | 776 |
| Detalles de la política | 777 |
| Versión de la política | 777 |
| Documento de política JSON | 777 |
| Más información | 777 |
| AmazonPrometheusScrapperServiceRolePolicy | 778 |
| Uso de la política | 778 |
| Información de la política | 778 |
| Versión de la política | 778 |
| Documento de política JSON | 778 |
| Más información | 780 |
| AmazonQFullAccess | 780 |
| Uso de la política | 781 |
| Información de la política | 781 |
| Versión de la política | 781 |
| Documento de política JSON | 781 |
| Más información | 781 |
| AmazonQLDBConsoleFullAccess | 782 |
| Uso de esta política | 782 |
| Detalles de la política | 782 |
| Versión de la política | 782 |
| Documento de política JSON | 782 |
| Más información | 784 |

| | |
|--|-----|
| AmazonQLDBFullAccess | 784 |
| Uso de esta política | 784 |
| Detalles de la política | 785 |
| Versión de la política | 785 |
| Documento de política JSON | 785 |
| Más información | 786 |
| AmazonQLDBReadOnly | 787 |
| Uso de esta política | 787 |
| Detalles de la política | 787 |
| Versión de la política | 787 |
| Documento de política JSON | 787 |
| Más información | 788 |
| AmazonRDSBetaServiceRolePolicy | 788 |
| Uso de esta política | 788 |
| Detalles de la política | 788 |
| Versión de la política | 789 |
| Documento de política JSON | 789 |
| Más información | 792 |
| AmazonRDSCustomInstanceProfileRolePolicy | 792 |
| Uso de la política | 792 |
| Información de la política | 792 |
| Versión de la política | 792 |
| Documento de política JSON | 793 |
| Más información | 800 |
| AmazonRDSCustomPreviewServiceRolePolicy | 800 |
| Uso de esta política | 800 |
| Detalles de la política | 800 |
| Versión de la política | 801 |
| Documento de política JSON | 801 |
| Más información | 816 |
| AmazonRDSCustomServiceRolePolicy | 817 |
| Uso de esta política | 817 |
| Detalles de la política | 817 |
| Versión de la política | 817 |
| Documento de política JSON | 817 |
| Más información | 834 |

| | |
|--|-----|
| AmazonRDSDDataFullAccess | 834 |
| Uso de esta política | 834 |
| Detalles de la política | 834 |
| Versión de la política | 835 |
| Documento de política JSON | 835 |
| Más información | 836 |
| AmazonRDSDirectoryServiceAccess | 836 |
| Uso de esta política | 836 |
| Detalles de la política | 836 |
| Versión de la política | 837 |
| Documento de política JSON | 837 |
| Más información | 837 |
| AmazonRDSEnhancedMonitoringRole | 838 |
| Uso de esta política | 838 |
| Detalles de la política | 838 |
| Versión de la política | 838 |
| Documento de política JSON | 838 |
| Más información | 839 |
| AmazonRDSFullAccess | 839 |
| Uso de la política | 839 |
| Información de la política | 839 |
| Versión de la política | 840 |
| Documento de política JSON | 840 |
| Más información | 842 |
| AmazonRDSPerformancelnsightsFullAccess | 842 |
| Uso de la política | 842 |
| Información de la política | 842 |
| Versión de la política | 843 |
| Documento de política JSON | 843 |
| Más información | 844 |
| AmazonRDSPerformancelnsightsReadOnly | 844 |
| Uso de la política | 845 |
| Información de la política | 845 |
| Versión de la política | 845 |
| Documento de política JSON | 845 |
| Más información | 847 |

| | |
|---|-----|
| AmazonRDSPreviewServiceRolePolicy | 847 |
| Uso de la política | 847 |
| Información de la política | 847 |
| Versión de la política | 848 |
| Documento de política JSON | 848 |
| Más información | 851 |
| AmazonRDSReadOnlyAccess | 851 |
| Uso de la política | 851 |
| Información de la política | 851 |
| Versión de la política | 852 |
| Documento de política JSON | 852 |
| Más información | 853 |
| AmazonRDSServiceRolePolicy | 853 |
| Uso de la política | 853 |
| Información de la política | 854 |
| Versión de la política | 854 |
| Documento de política JSON | 854 |
| Más información | 858 |
| AmazonRedshiftAllCommandsFullAccess | 858 |
| Uso de la política | 858 |
| Información de la política | 858 |
| Versión de la política | 859 |
| Documento de política JSON | 859 |
| Más información | 864 |
| AmazonRedshiftDataFullAccess | 864 |
| Uso de la política | 864 |
| Información de la política | 864 |
| Versión de la política | 865 |
| Documento de política JSON | 865 |
| Más información | 867 |
| AmazonRedshiftFullAccess | 867 |
| Uso de la política | 867 |
| Información de la política | 867 |
| Versión de la política | 867 |
| Documento de política JSON | 868 |
| Más información | 870 |

| | |
|---|-----|
| AmazonRedshiftQueryEditor | 870 |
| Uso de la política | 870 |
| Información de la política | 870 |
| Versión de la política | 870 |
| Documento de política JSON | 871 |
| Más información | 872 |
| AmazonRedshiftQueryEditorV2FullAccess | 873 |
| Uso de la política | 873 |
| Información de la política | 873 |
| Versión de la política | 873 |
| Documento de política JSON | 873 |
| Más información | 875 |
| AmazonRedshiftQueryEditorV2NoSharing | 875 |
| Uso de la política | 875 |
| Información de la política | 875 |
| Versión de la política | 876 |
| Documento de política JSON | 876 |
| Más información | 879 |
| AmazonRedshiftQueryEditorV2ReadSharing | 880 |
| Uso de la política | 880 |
| Información de la política | 880 |
| Versión de la política | 880 |
| Documento de política JSON | 880 |
| Más información | 885 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing | 885 |
| Uso de la política | 886 |
| Información de la política | 886 |
| Versión de la política | 886 |
| Documento de política JSON | 886 |
| Más información | 891 |
| AmazonRedshiftReadOnlyAccess | 891 |
| Uso de la política | 892 |
| Información de la política | 892 |
| Versión de la política | 892 |
| Documento de política JSON | 892 |
| Más información | 893 |

| | |
|---|-----|
| AmazonRedshiftServiceLinkedRolePolicy | 893 |
| Uso de la política | 893 |
| Información de la política | 893 |
| Versión de la política | 894 |
| Documento de política JSON | 894 |
| Más información | 899 |
| AmazonRekognitionCustomLabelsFullAccess | 899 |
| Uso de la política | 899 |
| Información de la política | 900 |
| Versión de la política | 900 |
| Documento de política JSON | 900 |
| Más información | 901 |
| AmazonRekognitionFullAccess | 901 |
| Uso de la política | 902 |
| Información de la política | 902 |
| Versión de la política | 902 |
| Documento de política JSON | 902 |
| Más información | 902 |
| AmazonRekognitionReadOnlyAccess | 903 |
| Uso de la política | 903 |
| Información de la política | 903 |
| Versión de la política | 903 |
| Documento de política JSON | 903 |
| Más información | 905 |
| AmazonRekognitionServiceRole | 905 |
| Uso de la política | 905 |
| Información de la política | 905 |
| Versión de la política | 905 |
| Documento de política JSON | 905 |
| Más información | 906 |
| AmazonRoute53AutoNamingFullAccess | 906 |
| Uso de la política | 907 |
| Información de la política | 907 |
| Versión de la política | 907 |
| Documento de política JSON | 907 |
| Más información | 908 |

| | |
|---|-----|
| AmazonRoute53AutoNamingReadOnlyAccess | 908 |
| Uso de la política | 908 |
| Información de la política | 908 |
| Versión de la política | 908 |
| Documento de política JSON | 909 |
| Más información | 909 |
| AmazonRoute53AutoNamingRegistrantAccess | 909 |
| Uso de la política | 909 |
| Información de la política | 910 |
| Versión de la política | 910 |
| Documento de política JSON | 910 |
| Más información | 911 |
| AmazonRoute53DomainsFullAccess | 911 |
| Uso de la política | 911 |
| Información de la política | 911 |
| Versión de la política | 911 |
| Documento de política JSON | 912 |
| Más información | 912 |
| AmazonRoute53DomainsReadOnlyAccess | 912 |
| Uso de la política | 912 |
| Información de la política | 912 |
| Versión de la política | 913 |
| Documento de política JSON | 913 |
| Más información | 913 |
| AmazonRoute53FullAccess | 914 |
| Uso de la política | 914 |
| Información de la política | 914 |
| Versión de la política | 914 |
| Documento de política JSON | 914 |
| Más información | 915 |
| AmazonRoute53ReadOnlyAccess | 915 |
| Uso de la política | 915 |
| Información de la política | 915 |
| Versión de la política | 916 |
| Documento de política JSON | 916 |
| Más información | 916 |

| | |
|--|-----|
| AmazonRoute53RecoveryClusterFullAccess | 917 |
| Uso de la política | 917 |
| Información de la política | 917 |
| Versión de la política | 917 |
| Documento de política JSON | 917 |
| Más información | 918 |
| AmazonRoute53RecoveryClusterReadOnlyAccess | 918 |
| Uso de la política | 918 |
| Información de la política | 918 |
| Versión de la política | 918 |
| Documento de política JSON | 918 |
| Más información | 919 |
| AmazonRoute53RecoveryControlConfigFullAccess | 919 |
| Uso de la política | 919 |
| Información de la política | 919 |
| Versión de la política | 920 |
| Documento de política JSON | 920 |
| Más información | 920 |
| AmazonRoute53RecoveryControlConfigReadOnlyAccess | 920 |
| Uso de la política | 921 |
| Información de la política | 921 |
| Versión de la política | 921 |
| Documento de política JSON | 921 |
| Más información | 922 |
| AmazonRoute53RecoveryReadinessFullAccess | 922 |
| Uso de la política | 922 |
| Información de la política | 922 |
| Versión de la política | 922 |
| Documento de política JSON | 923 |
| Más información | 923 |
| AmazonRoute53RecoveryReadinessReadOnlyAccess | 923 |
| Uso de la política | 923 |
| Información de la política | 924 |
| Versión de la política | 924 |
| Documento de política JSON | 924 |
| Más información | 925 |

| | |
|---|-----|
| AmazonRoute53ResolverFullAccess | 925 |
| Uso de la política | 925 |
| Información de la política | 925 |
| Versión de la política | 926 |
| Documento de política JSON | 926 |
| Más información | 926 |
| AmazonRoute53ResolverReadOnlyAccess | 927 |
| Uso de la política | 927 |
| Información de la política | 927 |
| Versión de la política | 927 |
| Documento de política JSON | 927 |
| Más información | 928 |
| AmazonS3FullAccess | 928 |
| Uso de la política | 928 |
| Información de la política | 928 |
| Versión de la política | 929 |
| Documento de política JSON | 929 |
| Más información | 929 |
| AmazonS3ObjectLambdaExecutionRolePolicy | 929 |
| Uso de la política | 930 |
| Información de la política | 930 |
| Versión de la política | 930 |
| Documento de política JSON | 930 |
| Más información | 931 |
| AmazonS3OutpostsFullAccess | 931 |
| Uso de la política | 931 |
| Información de la política | 931 |
| Versión de la política | 931 |
| Documento de política JSON | 931 |
| Más información | 932 |
| AmazonS3OutpostsReadOnlyAccess | 933 |
| Uso de la política | 933 |
| Información de la política | 933 |
| Versión de la política | 933 |
| Documento de política JSON | 933 |
| Más información | 934 |

| | |
|--|-----|
| AmazonS3ReadOnlyAccess | 935 |
| Uso de la política | 935 |
| Información de la política | 935 |
| Versión de la política | 935 |
| Documento de política JSON | 935 |
| Más información | 936 |
| AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy | 936 |
| Uso de la política | 936 |
| Información de la política | 936 |
| Versión de la política | 937 |
| Documento de política JSON | 937 |
| Más información | 947 |
| AmazonSageMakerCanvasAIServicesAccess | 947 |
| Uso de la política | 947 |
| Información de la política | 947 |
| Versión de la política | 948 |
| Documento de política JSON | 948 |
| Más información | 951 |
| AmazonSageMakerCanvasBedrockAccess | 951 |
| Uso de la política | 951 |
| Información de la política | 951 |
| Versión de la política | 951 |
| Documento de política JSON | 952 |
| Más información | 952 |
| AmazonSageMakerCanvasDataPrepFullAccess | 953 |
| Uso de la política | 953 |
| Información de la política | 953 |
| Versión de la política | 953 |
| Documento de política JSON | 953 |
| Más información | 960 |
| AmazonSageMakerCanvasDirectDeployAccess | 961 |
| Uso de la política | 961 |
| Información de la política | 961 |
| Versión de la política | 961 |
| Documento de política JSON | 961 |
| Más información | 962 |

| | |
|--|-----|
| AmazonSageMakerCanvasForecastAccess | 962 |
| Uso de la política | 962 |
| Información de la política | 963 |
| Versión de la política | 963 |
| Documento de política JSON | 963 |
| Más información | 964 |
| AmazonSageMakerCanvasFullAccess | 964 |
| Uso de la política | 964 |
| Información de la política | 964 |
| Versión de la política | 964 |
| Documento de política JSON | 965 |
| Más información | 973 |
| AmazonSageMakerClusterInstanceRolePolicy | 973 |
| Uso de la política | 973 |
| Información de la política | 973 |
| Versión de la política | 973 |
| Documento de política JSON | 973 |
| Más información | 975 |
| AmazonSageMakerCoreServiceRolePolicy | 975 |
| Uso de la política | 976 |
| Información de la política | 976 |
| Versión de la política | 976 |
| Documento de política JSON | 976 |
| Más información | 977 |
| AmazonSageMakerEdgeDeviceFleetPolicy | 977 |
| Uso de la política | 977 |
| Información de la política | 977 |
| Versión de la política | 978 |
| Documento de política JSON | 978 |
| Más información | 980 |
| AmazonSageMakerFeatureStoreAccess | 980 |
| Uso de la política | 980 |
| Información de la política | 980 |
| Versión de la política | 980 |
| Documento de política JSON | 981 |
| Más información | 982 |

| | |
|---|------|
| AmazonSageMakerFullAccess | 982 |
| Uso de la política | 982 |
| Información de la política | 982 |
| Versión de la política | 982 |
| Documento de política JSON | 982 |
| Más información | 998 |
| AmazonSageMakerGeospatialExecutionRole | 998 |
| Uso de la política | 998 |
| Información de la política | 999 |
| Versión de la política | 999 |
| Documento de política JSON | 999 |
| Más información | 1000 |
| AmazonSageMakerGeospatialFullAccess | 1000 |
| Uso de la política | 1000 |
| Información de la política | 1000 |
| Versión de la política | 1001 |
| Documento de política JSON | 1001 |
| Más información | 1001 |
| AmazonSageMakerGroundTruthExecution | 1002 |
| Uso de la política | 1002 |
| Información de la política | 1002 |
| Versión de la política | 1002 |
| Documento de política JSON | 1002 |
| Más información | 1006 |
| AmazonSageMakerMechanicalTurkAccess | 1006 |
| Uso de la política | 1006 |
| Información de la política | 1006 |
| Versión de la política | 1006 |
| Documento de política JSON | 1007 |
| Más información | 1007 |
| AmazonSageMakerModelGovernanceUseAccess | 1007 |
| Uso de la política | 1008 |
| Información de la política | 1008 |
| Versión de la política | 1008 |
| Documento de política JSON | 1008 |
| Más información | 1010 |

| | |
|---|------|
| AmazonSageMakerModelRegistryFullAccess | 1010 |
| Uso de la política | 1010 |
| Información de la política | 1010 |
| Versión de la política | 1011 |
| Documento de política JSON | 1011 |
| Más información | 1014 |
| AmazonSageMakerNotebooksServiceRolePolicy | 1014 |
| Uso de la política | 1014 |
| Información de la política | 1014 |
| Versión de la política | 1014 |
| Documento de política JSON | 1015 |
| Más información | 1018 |
| AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy | 1018 |
| Uso de la política | 1018 |
| Información de la política | 1018 |
| Versión de la política | 1018 |
| Documento de política JSON | 1019 |
| Más información | 1020 |
| AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy | 1020 |
| Uso de la política | 1020 |
| Información de la política | 1020 |
| Versión de la política | 1020 |
| Documento de política JSON | 1021 |
| Más información | 1024 |
| AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy | 1024 |
| Uso de la política | 1025 |
| Información de la política | 1025 |
| Versión de la política | 1025 |
| Documento de política JSON | 1025 |
| Más información | 1026 |
| AmazonSageMakerPipelinesIntegrations | 1026 |
| Uso de la política | 1026 |
| Información de la política | 1026 |
| Versión de la política | 1026 |
| Documento de política JSON | 1027 |
| Más información | 1028 |

| | |
|--|------|
| AmazonSageMakerReadOnly | 1029 |
| Uso de la política | 1029 |
| Información de la política | 1029 |
| Versión de la política | 1029 |
| Documento de política JSON | 1029 |
| Más información | 1030 |
| AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy | 1031 |
| Uso de la política | 1031 |
| Información de la política | 1031 |
| Versión de la política | 1031 |
| Documento de política JSON | 1032 |
| Más información | 1032 |
| AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy | 1033 |
| Uso de la política | 1033 |
| Información de la política | 1033 |
| Versión de la política | 1033 |
| Documento de política JSON | 1033 |
| Más información | 1040 |
| AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy | 1040 |
| Uso de la política | 1041 |
| Información de la política | 1041 |
| Versión de la política | 1041 |
| Documento de política JSON | 1041 |
| Más información | 1050 |
| AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy | 1051 |
| Uso de la política | 1051 |
| Información de la política | 1051 |
| Versión de la política | 1051 |
| Documento de política JSON | 1051 |
| Más información | 1053 |
| AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy | 1053 |
| Uso de la política | 1053 |
| Información de la política | 1054 |
| Versión de la política | 1054 |
| Documento de política JSON | 1054 |
| Más información | 1054 |

| | |
|--|------|
| AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy | 1055 |
| Uso de la política | 1055 |
| Información de la política | 1055 |
| Versión de la política | 1055 |
| Documento de política JSON | 1055 |
| Más información | 1056 |
| AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy | 1056 |
| Uso de la política | 1056 |
| Información de la política | 1056 |
| Versión de la política | 1057 |
| Documento de política JSON | 1057 |
| Más información | 1059 |
| AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy | 1059 |
| Uso de la política | 1059 |
| Información de la política | 1059 |
| Versión de la política | 1060 |
| Documento de política JSON | 1060 |
| Más información | 1069 |
| AmazonSecurityLakeAdministrator | 1070 |
| Uso de la política | 1070 |
| Información de la política | 1070 |
| Versión de la política | 1070 |
| Documento de política JSON | 1070 |
| Más información | 1081 |
| AmazonSecurityLakeMetastoreManager | 1082 |
| Uso de la política | 1082 |
| Información de la política | 1082 |
| Versión de la política | 1082 |
| Documento de política JSON | 1082 |
| Más información | 1084 |
| AmazonSecurityLakePermissionsBoundary | 1084 |
| Uso de la política | 1085 |
| Información de la política | 1085 |
| Versión de la política | 1085 |
| Documento de política JSON | 1085 |
| Más información | 1088 |

| | |
|----------------------------------|------|
| AmazonSESEFullAccess | 1088 |
| Uso de la política | 1089 |
| Información de la política | 1089 |
| Versión de la política | 1089 |
| Documento de política JSON | 1089 |
| Más información | 1089 |
| AmazonSESReadOnlyAccess | 1090 |
| Uso de la política | 1090 |
| Información de la política | 1090 |
| Versión de la política | 1090 |
| Documento de política JSON | 1090 |
| Más información | 1091 |
| AmazonSNSFullAccess | 1091 |
| Uso de la política | 1091 |
| Información de la política | 1091 |
| Versión de la política | 1091 |
| Documento de política JSON | 1092 |
| Más información | 1092 |
| AmazonSNSReadOnlyAccess | 1092 |
| Uso de la política | 1092 |
| Información de la política | 1093 |
| Versión de la política | 1093 |
| Documento de política JSON | 1093 |
| Más información | 1093 |
| AmazonSNSRole | 1094 |
| Uso de la política | 1094 |
| Información de la política | 1094 |
| Versión de la política | 1094 |
| Documento de política JSON | 1094 |
| Más información | 1095 |
| AmazonSQSFullAccess | 1095 |
| Uso de la política | 1095 |
| Información de la política | 1095 |
| Versión de la política | 1095 |
| Documento de política JSON | 1096 |
| Más información | 1096 |

| | |
|---|------|
| AmazonSQSReadOnlyAccess | 1096 |
| Uso de la política | 1096 |
| Información de la política | 1097 |
| Versión de la política | 1097 |
| Documento de política JSON | 1097 |
| Más información | 1097 |
| AmazonSSMAutomationApproverAccess | 1098 |
| Uso de la política | 1098 |
| Información de la política | 1098 |
| Versión de la política | 1098 |
| Documento de política JSON | 1098 |
| Más información | 1099 |
| AmazonSSMAutomationRole | 1099 |
| Uso de la política | 1099 |
| Información de la política | 1099 |
| Versión de la política | 1100 |
| Documento de política JSON | 1100 |
| Más información | 1101 |
| AmazonSSMDirectoryServiceAccess | 1101 |
| Uso de la política | 1102 |
| Información de la política | 1102 |
| Versión de la política | 1102 |
| Documento de política JSON | 1102 |
| Más información | 1102 |
| AmazonSSMFullAccess | 1103 |
| Uso de la política | 1103 |
| Información de la política | 1103 |
| Versión de la política | 1103 |
| Documento de política JSON | 1103 |
| Más información | 1105 |
| AmazonSSMMaintenanceWindowRole | 1105 |
| Uso de la política | 1105 |
| Información de la política | 1105 |
| Versión de la política | 1105 |
| Documento de política JSON | 1105 |
| Más información | 1107 |

| | |
|--|------|
| AmazonSSMManagedEC2InstanceDefaultPolicy | 1107 |
| Uso de la política | 1107 |
| Información de la política | 1107 |
| Versión de la política | 1108 |
| Documento de política JSON | 1108 |
| Más información | 1109 |
| AmazonSSMManagedInstanceCore | 1109 |
| Uso de la política | 1109 |
| Información de la política | 1109 |
| Versión de la política | 1110 |
| Documento de política JSON | 1110 |
| Más información | 1111 |
| AmazonSSMPatchAssociation | 1111 |
| Uso de la política | 1111 |
| Información de la política | 1111 |
| Versión de la política | 1112 |
| Documento de política JSON | 1112 |
| Más información | 1113 |
| AmazonSSMReadOnlyAccess | 1113 |
| Uso de la política | 1113 |
| Información de la política | 1113 |
| Versión de la política | 1113 |
| Documento de política JSON | 1113 |
| Más información | 1114 |
| AmazonSSMServiceRolePolicy | 1114 |
| Uso de la política | 1114 |
| Información de la política | 1114 |
| Versión de la política | 1115 |
| Documento de política JSON | 1115 |
| Más información | 1120 |
| AmazonSumerianFullAccess | 1120 |
| Uso de la política | 1120 |
| Información de la política | 1120 |
| Versión de la política | 1120 |
| Documento de política JSON | 1121 |
| Más información | 1121 |

| | |
|---|------|
| AmazonTextractFullAccess | 1121 |
| Uso de la política | 1121 |
| Información de la política | 1122 |
| Versión de la política | 1122 |
| Documento de política JSON | 1122 |
| Más información | 1122 |
| AmazonTextractServiceRole | 1123 |
| Uso de la política | 1123 |
| Información de la política | 1123 |
| Versión de la política | 1123 |
| Documento de política JSON | 1123 |
| Más información | 1124 |
| AmazonTimestreamConsoleFullAccess | 1124 |
| Uso de la política | 1124 |
| Información de la política | 1124 |
| Versión de la política | 1124 |
| Documento de política JSON | 1125 |
| Más información | 1126 |
| AmazonTimestreamFullAccess | 1127 |
| Uso de la política | 1127 |
| Información de la política | 1127 |
| Versión de la política | 1127 |
| Documento de política JSON | 1127 |
| Más información | 1128 |
| AmazonTimestreamInfluxDBFullAccess | 1129 |
| Uso de la política | 1129 |
| Información de la política | 1129 |
| Versión de la política | 1129 |
| Documento de política JSON | 1129 |
| Más información | 1131 |
| AmazonTimestreamInfluxDBServiceRolePolicy | 1131 |
| Uso de la política | 1132 |
| Información de la política | 1132 |
| Versión de la política | 1132 |
| Documento de política JSON | 1132 |
| Más información | 1135 |

| | |
|---|------|
| AmazonTimestreamReadOnlyAccess | 1135 |
| Uso de la política | 1135 |
| Información de la política | 1135 |
| Versión de la política | 1135 |
| Documento de política JSON | 1136 |
| Más información | 1136 |
| AmazonTranscribeFullAccess | 1137 |
| Uso de la política | 1137 |
| Información de la política | 1137 |
| Versión de la política | 1137 |
| Documento de política JSON | 1137 |
| Más información | 1138 |
| AmazonTranscribeReadOnlyAccess | 1138 |
| Uso de la política | 1138 |
| Información de la política | 1138 |
| Versión de la política | 1138 |
| Documento de política JSON | 1139 |
| Más información | 1139 |
| AmazonVPCCrossAccountNetworkInterfaceOperations | 1139 |
| Uso de la política | 1139 |
| Información de la política | 1140 |
| Versión de la política | 1140 |
| Documento de política JSON | 1140 |
| Más información | 1141 |
| AmazonVPCFullAccess | 1142 |
| Uso de la política | 1142 |
| Información de la política | 1142 |
| Versión de la política | 1142 |
| Documento de política JSON | 1142 |
| Más información | 1146 |
| AmazonVPCNetworkAccessAnalyzerFullAccessPolicy | 1146 |
| Uso de la política | 1147 |
| Información de la política | 1147 |
| Versión de la política | 1147 |
| Documento de política JSON | 1147 |
| Más información | 1150 |

| | |
|--|------|
| AmazonVPCReachabilityAnalyzerFullAccessPolicy | 1151 |
| Uso de la política | 1151 |
| Información de la política | 1151 |
| Versión de la política | 1151 |
| Documento de política JSON | 1151 |
| Más información | 1154 |
| AmazonVPCReachabilityAnalyzerPathComponentReadPolicy | 1154 |
| Uso de la política | 1155 |
| Información de la política | 1155 |
| Versión de la política | 1155 |
| Documento de política JSON | 1155 |
| Más información | 1156 |
| AmazonVPCReadOnlyAccess | 1156 |
| Uso de la política | 1156 |
| Información de la política | 1156 |
| Versión de la política | 1156 |
| Documento de política JSON | 1156 |
| Más información | 1158 |
| AmazonWorkDocsFullAccess | 1158 |
| Uso de la política | 1158 |
| Información de la política | 1158 |
| Versión de la política | 1158 |
| Documento de política JSON | 1159 |
| Más información | 1159 |
| AmazonWorkDocsReadOnlyAccess | 1159 |
| Uso de la política | 1159 |
| Información de la política | 1160 |
| Versión de la política | 1160 |
| Documento de política JSON | 1160 |
| Más información | 1160 |
| AmazonWorkMailEventsServiceRolePolicy | 1161 |
| Uso de la política | 1161 |
| Información de la política | 1161 |
| Versión de la política | 1161 |
| Documento de política JSON | 1161 |
| Más información | 1162 |

| | |
|---|------|
| AmazonWorkMailFullAccess | 1162 |
| Uso de la política | 1162 |
| Información de la política | 1162 |
| Versión de la política | 1162 |
| Documento de política JSON | 1163 |
| Más información | 1165 |
| AmazonWorkMailMessageFlowFullAccess | 1165 |
| Uso de la política | 1165 |
| Información de la política | 1165 |
| Versión de la política | 1165 |
| Documento de política JSON | 1166 |
| Más información | 1166 |
| AmazonWorkMailMessageFlowReadOnlyAccess | 1166 |
| Uso de la política | 1166 |
| Información de la política | 1166 |
| Versión de la política | 1167 |
| Documento de política JSON | 1167 |
| Más información | 1167 |
| AmazonWorkMailReadOnlyAccess | 1167 |
| Uso de la política | 1168 |
| Información de la política | 1168 |
| Versión de la política | 1168 |
| Documento de política JSON | 1168 |
| Más información | 1169 |
| AmazonWorkSpacesAdmin | 1169 |
| Uso de la política | 1169 |
| Información de la política | 1169 |
| Versión de la política | 1169 |
| Documento de política JSON | 1170 |
| Más información | 1170 |
| AmazonWorkSpacesApplicationManagerAdminAccess | 1171 |
| Uso de la política | 1171 |
| Información de la política | 1171 |
| Versión de la política | 1171 |
| Documento de política JSON | 1171 |
| Más información | 1172 |

| | |
|--|------|
| AmazonWorkspacesPCAAccess | 1172 |
| Uso de la política | 1172 |
| Información de la política | 1172 |
| Versión de la política | 1172 |
| Documento de política JSON | 1173 |
| Más información | 1173 |
| AmazonWorkSpacesSelfServiceAccess | 1174 |
| Uso de la política | 1174 |
| Información de la política | 1174 |
| Versión de la política | 1174 |
| Documento de política JSON | 1174 |
| Más información | 1175 |
| AmazonWorkSpacesServiceAccess | 1175 |
| Uso de la política | 1175 |
| Información de la política | 1175 |
| Versión de la política | 1175 |
| Documento de política JSON | 1176 |
| Más información | 1176 |
| AmazonWorkSpacesWebReadOnly | 1176 |
| Uso de la política | 1176 |
| Información de la política | 1176 |
| Versión de la política | 1177 |
| Documento de política JSON | 1177 |
| Más información | 1178 |
| AmazonWorkSpacesWebServiceRolePolicy | 1178 |
| Uso de la política | 1178 |
| Información de la política | 1178 |
| Versión de la política | 1179 |
| Documento de política JSON | 1179 |
| Más información | 1181 |
| AmazonZocaloFullAccess | 1181 |
| Uso de la política | 1181 |
| Información de la política | 1181 |
| Versión de la política | 1182 |
| Documento de política JSON | 1182 |
| Más información | 1183 |

| | |
|--|------|
| AmazonZocaloReadOnlyAccess | 1183 |
| Uso de la política | 1183 |
| Información de la política | 1183 |
| Versión de la política | 1183 |
| Documento de política JSON | 1184 |
| Más información | 1184 |
| AmplifyBackendDeployFullAccess | 1184 |
| Uso de la política | 1184 |
| Información de la política | 1185 |
| Versión de la política | 1185 |
| Documento de política JSON | 1185 |
| Más información | 1188 |
| APIGatewayServiceRolePolicy | 1188 |
| Uso de la política | 1188 |
| Información de la política | 1189 |
| Versión de la política | 1189 |
| Documento de política JSON | 1189 |
| Más información | 1191 |
| AppIntegrationsServiceLinkedRolePolicy | 1191 |
| Uso de la política | 1192 |
| Información de la política | 1192 |
| Versión de la política | 1192 |
| Documento de política JSON | 1192 |
| Más información | 1194 |
| ApplicationAutoScalingForAmazonAppStreamAccess | 1194 |
| Uso de la política | 1194 |
| Información de la política | 1194 |
| Versión de la política | 1194 |
| Documento de política JSON | 1195 |
| Más información | 1195 |
| ApplicationDiscoveryServiceContinuousExportServiceRolePolicy | 1196 |
| Uso de la política | 1196 |
| Información de la política | 1196 |
| Versión de la política | 1196 |
| Documento de política JSON | 1196 |
| Más información | 1198 |

| | |
|--|------|
| AppRunnerNetworkingServiceRolePolicy | 1198 |
| Uso de la política | 1199 |
| Información de la política | 1199 |
| Versión de la política | 1199 |
| Documento de política JSON | 1199 |
| Más información | 1200 |
| AppRunnerServiceRolePolicy | 1201 |
| Uso de la política | 1201 |
| Información de la política | 1201 |
| Versión de la política | 1201 |
| Documento de política JSON | 1201 |
| Más información | 1202 |
| AutoScalingConsoleFullAccess | 1202 |
| Uso de la política | 1202 |
| Información de la política | 1203 |
| Versión de la política | 1203 |
| Documento de política JSON | 1203 |
| Más información | 1205 |
| AutoScalingConsoleReadOnlyAccess | 1205 |
| Uso de la política | 1205 |
| Información de la política | 1205 |
| Versión de la política | 1205 |
| Documento de política JSON | 1206 |
| Más información | 1207 |
| AutoScalingFullAccess | 1207 |
| Uso de la política | 1207 |
| Información de la política | 1207 |
| Versión de la política | 1207 |
| Documento de política JSON | 1208 |
| Más información | 1209 |
| AutoScalingNotificationAccessRole | 1209 |
| Uso de la política | 1209 |
| Información de la política | 1209 |
| Versión de la política | 1210 |
| Documento de política JSON | 1210 |
| Más información | 1210 |

| | |
|--|------|
| AutoScalingReadOnlyAccess | 1210 |
| Uso de la política | 1211 |
| Información de la política | 1211 |
| Versión de la política | 1211 |
| Documento de política JSON | 1211 |
| Más información | 1211 |
| AutoScalingServiceRolePolicy | 1212 |
| Uso de la política | 1212 |
| Información de la política | 1212 |
| Versión de la política | 1212 |
| Documento de política JSON | 1212 |
| Más información | 1215 |
| AWS_ConfigRole | 1215 |
| Uso de la política | 1215 |
| Información de la política | 1216 |
| Versión de la política | 1216 |
| Documento de política JSON | 1216 |
| Más información | 1247 |
| AWSAccountActivityAccess | 1247 |
| Uso de la política | 1247 |
| Información de la política | 1247 |
| Versión de la política | 1247 |
| Documento de política JSON | 1248 |
| Más información | 1248 |
| AWSAccountManagementFullAccess | 1249 |
| Uso de la política | 1249 |
| Información de la política | 1249 |
| Versión de la política | 1249 |
| Documento de política JSON | 1249 |
| Más información | 1250 |
| AWSAccountManagementReadOnlyAccess | 1250 |
| Uso de la política | 1250 |
| Información de la política | 1250 |
| Versión de la política | 1250 |
| Documento de política JSON | 1251 |
| Más información | 1251 |

| | |
|---|------|
| AWSAccountUsageReportAccess | 1251 |
| Uso de la política | 1251 |
| Información de la política | 1251 |
| Versión de la política | 1252 |
| Documento de política JSON | 1252 |
| Más información | 1252 |
| AWSAgentlessDiscoveryService | 1253 |
| Uso de la política | 1253 |
| Información de la política | 1253 |
| Versión de la política | 1253 |
| Documento de política JSON | 1253 |
| Más información | 1255 |
| AWSAppFabricFullAccess | 1255 |
| Uso de la política | 1255 |
| Información de la política | 1256 |
| Versión de la política | 1256 |
| Documento de política JSON | 1256 |
| Más información | 1257 |
| AWSAppFabricReadOnlyAccess | 1258 |
| Uso de la política | 1258 |
| Información de la política | 1258 |
| Versión de la política | 1258 |
| Documento de política JSON | 1258 |
| Más información | 1259 |
| AWSAppFabricServiceRolePolicy | 1259 |
| Uso de la política | 1259 |
| Información de la política | 1259 |
| Versión de la política | 1259 |
| Documento de política JSON | 1260 |
| Más información | 1261 |
| AWSApplicationAutoscalingAppStreamFleetPolicy | 1261 |
| Uso de la política | 1261 |
| Información de la política | 1261 |
| Versión de la política | 1261 |
| Documento de política JSON | 1262 |
| Más información | 1262 |

| | |
|--|------|
| AWSApplicationAutoscalingCassandraTablePolicy | 1262 |
| Uso de la política | 1263 |
| Información de la política | 1263 |
| Versión de la política | 1263 |
| Documento de política JSON | 1263 |
| Más información | 1264 |
| AWSApplicationAutoscalingComprehendEndpointPolicy | 1264 |
| Uso de la política | 1264 |
| Información de la política | 1264 |
| Versión de la política | 1264 |
| Documento de política JSON | 1265 |
| Más información | 1265 |
| AWSApplicationAutoScalingCustomResourcePolicy | 1265 |
| Uso de la política | 1266 |
| Información de la política | 1266 |
| Versión de la política | 1266 |
| Documento de política JSON | 1266 |
| Más información | 1267 |
| AWSApplicationAutoscalingDynamoDBTablePolicy | 1267 |
| Uso de la política | 1267 |
| Información de la política | 1267 |
| Versión de la política | 1267 |
| Documento de política JSON | 1268 |
| Más información | 1268 |
| AWSApplicationAutoscalingEC2SpotFleetRequestPolicy | 1268 |
| Uso de la política | 1268 |
| Información de la política | 1268 |
| Versión de la política | 1269 |
| Documento de política JSON | 1269 |
| Más información | 1269 |
| AWSApplicationAutoscalingECSServicePolicy | 1270 |
| Uso de la política | 1270 |
| Información de la política | 1270 |
| Versión de la política | 1270 |
| Documento de política JSON | 1270 |
| Más información | 1271 |

| | |
|--|------|
| AWSApplicationAutoscalingElastiCacheRGPolicy | 1271 |
| Uso de la política | 1271 |
| Información de la política | 1271 |
| Versión de la política | 1271 |
| Documento de política JSON | 1272 |
| Más información | 1272 |
| AWSApplicationAutoscalingEMRInstanceGroupPolicy | 1273 |
| Uso de la política | 1273 |
| Información de la política | 1273 |
| Versión de la política | 1273 |
| Documento de política JSON | 1273 |
| Más información | 1274 |
| AWSApplicationAutoscalingKafkaClusterPolicy | 1274 |
| Uso de la política | 1274 |
| Información de la política | 1274 |
| Versión de la política | 1274 |
| Documento de política JSON | 1275 |
| Más información | 1275 |
| AWSApplicationAutoscalingLambdaConcurrencyPolicy | 1275 |
| Uso de la política | 1276 |
| Información de la política | 1276 |
| Versión de la política | 1276 |
| Documento de política JSON | 1276 |
| Más información | 1277 |
| AWSApplicationAutoscalingNeptuneClusterPolicy | 1277 |
| Uso de la política | 1277 |
| Información de la política | 1277 |
| Versión de la política | 1277 |
| Documento de política JSON | 1278 |
| Más información | 1279 |
| AWSApplicationAutoscalingRDSClusterPolicy | 1279 |
| Uso de la política | 1279 |
| Información de la política | 1280 |
| Versión de la política | 1280 |
| Documento de política JSON | 1280 |
| Más información | 1281 |

| | |
|--|------|
| AWSApplicationAutoscalingSageMakerEndpointPolicy | 1281 |
| Uso de la política | 1281 |
| Información de la política | 1281 |
| Versión de la política | 1282 |
| Documento de política JSON | 1282 |
| Más información | 1283 |
| AWSApplicationDiscoveryAgentAccess | 1283 |
| Uso de la política | 1283 |
| Información de la política | 1283 |
| Versión de la política | 1283 |
| Documento de política JSON | 1283 |
| Más información | 1284 |
| AWSApplicationDiscoveryAgentlessCollectorAccess | 1284 |
| Uso de la política | 1284 |
| Información de la política | 1284 |
| Versión de la política | 1285 |
| Documento de política JSON | 1285 |
| Más información | 1286 |
| AWSApplicationDiscoveryServiceFullAccess | 1286 |
| Uso de la política | 1286 |
| Información de la política | 1286 |
| Versión de la política | 1287 |
| Documento de política JSON | 1287 |
| Más información | 1288 |
| AWSApplicationMigrationAgentInstallationPolicy | 1289 |
| Uso de la política | 1289 |
| Información de la política | 1289 |
| Versión de la política | 1289 |
| Documento de política JSON | 1289 |
| Más información | 1290 |
| AWSApplicationMigrationAgentPolicy | 1290 |
| Uso de la política | 1291 |
| Información de la política | 1291 |
| Versión de la política | 1291 |
| Documento de política JSON | 1291 |
| Más información | 1292 |

| | |
|---|------|
| AWSApplicationMigrationAgentPolicy_v2 | 1292 |
| Uso de la política | 1292 |
| Información de la política | 1293 |
| Versión de la política | 1293 |
| Documento de política JSON | 1293 |
| Más información | 1294 |
| AWSApplicationMigrationConversionServerPolicy | 1294 |
| Uso de la política | 1294 |
| Información de la política | 1294 |
| Versión de la política | 1294 |
| Documento de política JSON | 1295 |
| Más información | 1295 |
| AWSApplicationMigrationEC2Access | 1295 |
| Uso de la política | 1296 |
| Información de la política | 1296 |
| Versión de la política | 1296 |
| Documento de política JSON | 1296 |
| Más información | 1304 |
| AWSApplicationMigrationFullAccess | 1304 |
| Uso de la política | 1304 |
| Información de la política | 1304 |
| Versión de la política | 1304 |
| Documento de política JSON | 1305 |
| Más información | 1310 |
| AWSApplicationMigrationMGHAccess | 1310 |
| Uso de la política | 1310 |
| Información de la política | 1310 |
| Versión de la política | 1311 |
| Documento de política JSON | 1311 |
| Más información | 1311 |
| AWSApplicationMigrationReadOnlyAccess | 1312 |
| Uso de la política | 1312 |
| Información de la política | 1312 |
| Versión de la política | 1312 |
| Documento de política JSON | 1312 |
| Más información | 1313 |

| | |
|---|------|
| AWSApplicationMigrationReplicationServerPolicy | 1314 |
| Uso de la política | 1314 |
| Información de la política | 1314 |
| Versión de la política | 1314 |
| Documento de política JSON | 1315 |
| Más información | 1316 |
| AWSApplicationMigrationServiceEc2InstancePolicy | 1317 |
| Uso de la política | 1317 |
| Información de la política | 1317 |
| Versión de la política | 1317 |
| Documento de política JSON | 1317 |
| Más información | 1318 |
| AWSApplicationMigrationServiceRolePolicy | 1319 |
| Uso de la política | 1319 |
| Información de la política | 1319 |
| Versión de la política | 1319 |
| Documento de política JSON | 1319 |
| Más información | 1326 |
| AWSApplicationMigrationSSMAccess | 1327 |
| Uso de la política | 1327 |
| Información de la política | 1327 |
| Versión de la política | 1327 |
| Documento de política JSON | 1327 |
| Más información | 1329 |
| AWSApplicationMigrationVCenterClientPolicy | 1329 |
| Uso de la política | 1330 |
| Información de la política | 1330 |
| Versión de la política | 1330 |
| Documento de política JSON | 1330 |
| Más información | 1331 |
| AWSAppMeshEnvoyAccess | 1331 |
| Uso de la política | 1331 |
| Información de la política | 1331 |
| Versión de la política | 1331 |
| Documento de política JSON | 1332 |
| Más información | 1332 |

| | |
|--|------|
| AWSAppMeshFullAccess | 1332 |
| Uso de la política | 1332 |
| Información de la política | 1333 |
| Versión de la política | 1333 |
| Documento de política JSON | 1333 |
| Más información | 1334 |
| AWSAppMeshPreviewEnvoyAccess | 1335 |
| Uso de la política | 1335 |
| Información de la política | 1335 |
| Versión de la política | 1335 |
| Documento de política JSON | 1335 |
| Más información | 1336 |
| AWSAppMeshPreviewServiceRolePolicy | 1336 |
| Uso de la política | 1336 |
| Información de la política | 1336 |
| Versión de la política | 1336 |
| Documento de política JSON | 1337 |
| Más información | 1337 |
| AWSAppMeshReadOnly | 1337 |
| Uso de la política | 1337 |
| Información de la política | 1338 |
| Versión de la política | 1338 |
| Documento de política JSON | 1338 |
| Más información | 1339 |
| AWSAppMeshServiceRolePolicy | 1339 |
| Uso de la política | 1339 |
| Información de la política | 1339 |
| Versión de la política | 1340 |
| Documento de política JSON | 1340 |
| Más información | 1340 |
| AWSAppRunnerFullAccess | 1341 |
| Uso de la política | 1341 |
| Información de la política | 1341 |
| Versión de la política | 1341 |
| Documento de política JSON | 1341 |
| Más información | 1342 |

| | |
|---|------|
| AWSAppRunnerReadOnlyAccess | 1342 |
| Uso de la política | 1342 |
| Información de la política | 1343 |
| Versión de la política | 1343 |
| Documento de política JSON | 1343 |
| Más información | 1343 |
| AWSAppRunnerServicePolicyForECRAccess | 1344 |
| Uso de la política | 1344 |
| Información de la política | 1344 |
| Versión de la política | 1344 |
| Documento de política JSON | 1344 |
| Más información | 1345 |
| AWSAppSyncAdministrator | 1345 |
| Uso de la política | 1345 |
| Información de la política | 1345 |
| Versión de la política | 1346 |
| Documento de política JSON | 1346 |
| Más información | 1347 |
| AWSAppSyncInvokeFullAccess | 1347 |
| Uso de la política | 1347 |
| Información de la política | 1347 |
| Versión de la política | 1348 |
| Documento de política JSON | 1348 |
| Más información | 1348 |
| AWSAppSyncPushToCloudWatchLogs | 1348 |
| Uso de la política | 1349 |
| Información de la política | 1349 |
| Versión de la política | 1349 |
| Documento de política JSON | 1349 |
| Más información | 1350 |
| AWSAppSyncSchemaAuthor | 1350 |
| Uso de la política | 1350 |
| Información de la política | 1350 |
| Versión de la política | 1350 |
| Documento de política JSON | 1350 |
| Más información | 1352 |

| | |
|--|------|
| AWSAppSyncServiceRolePolicy | 1352 |
| Uso de la política | 1352 |
| Información de la política | 1352 |
| Versión de la política | 1352 |
| Documento de política JSON | 1352 |
| Más información | 1353 |
| AWSArtifactAccountSync | 1353 |
| Uso de la política | 1353 |
| Información de la política | 1353 |
| Versión de la política | 1354 |
| Documento de política JSON | 1354 |
| Más información | 1354 |
| AWSArtifactReportsReadOnlyAccess | 1354 |
| Uso de la política | 1355 |
| Información de la política | 1355 |
| Versión de la política | 1355 |
| Documento de política JSON | 1355 |
| Más información | 1356 |
| AWSArtifactServiceRolePolicy | 1356 |
| Uso de la política | 1356 |
| Información de la política | 1356 |
| Versión de la política | 1356 |
| Documento de política JSON | 1357 |
| Más información | 1357 |
| AWSAuditManagerAdministratorAccess | 1357 |
| Uso de la política | 1357 |
| Información de la política | 1357 |
| Versión de la política | 1358 |
| Documento de política JSON | 1358 |
| Más información | 1362 |
| AWSAuditManagerServiceRolePolicy | 1362 |
| Uso de la política | 1362 |
| Información de la política | 1362 |
| Versión de la política | 1362 |
| Documento de política JSON | 1363 |
| Más información | 1367 |

| | |
|--|------|
| AWSAutoScalingPlansEC2AutoScalingPolicy | 1367 |
| Uso de la política | 1367 |
| Información de la política | 1367 |
| Versión de la política | 1368 |
| Documento de política JSON | 1368 |
| Más información | 1368 |
| AWSBackupAuditAccess | 1369 |
| Uso de la política | 1369 |
| Información de la política | 1369 |
| Versión de la política | 1369 |
| Documento de política JSON | 1369 |
| Más información | 1371 |
| AWSBackupDataTransferAccess | 1371 |
| Uso de la política | 1371 |
| Información de la política | 1371 |
| Versión de la política | 1371 |
| Documento de política JSON | 1372 |
| Más información | 1372 |
| AWSBackupFullAccess | 1372 |
| Uso de la política | 1373 |
| Información de la política | 1373 |
| Versión de la política | 1373 |
| Documento de política JSON | 1373 |
| Más información | 1383 |
| AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync | 1383 |
| Uso de la política | 1383 |
| Información de la política | 1383 |
| Versión de la política | 1384 |
| Documento de política JSON | 1384 |
| Más información | 1384 |
| AWSBackupOperatorAccess | 1385 |
| Uso de la política | 1385 |
| Información de la política | 1385 |
| Versión de la política | 1385 |
| Documento de política JSON | 1385 |
| Más información | 1392 |

| | |
|---|------|
| AWSBackupOrganizationAdminAccess | 1392 |
| Uso de la política | 1392 |
| Información de la política | 1393 |
| Versión de la política | 1393 |
| Documento de política JSON | 1393 |
| Más información | 1395 |
| AWSBackupRestoreAccessForSAPHANA | 1395 |
| Uso de la política | 1395 |
| Información de la política | 1395 |
| Versión de la política | 1396 |
| Documento de política JSON | 1396 |
| Más información | 1397 |
| AWSBackupServiceLinkedRolePolicyForBackup | 1397 |
| Uso de la política | 1397 |
| Información de la política | 1397 |
| Versión de la política | 1397 |
| Documento de política JSON | 1398 |
| Más información | 1405 |
| AWSBackupServiceLinkedRolePolicyForBackupTest | 1406 |
| Uso de la política | 1406 |
| Información de la política | 1406 |
| Versión de la política | 1406 |
| Documento de política JSON | 1406 |
| Más información | 1407 |
| AWSBackupServiceRolePolicyForBackup | 1407 |
| Uso de la política | 1407 |
| Información de la política | 1407 |
| Versión de la política | 1408 |
| Documento de política JSON | 1408 |
| Más información | 1418 |
| AWSBackupServiceRolePolicyForRestores | 1419 |
| Uso de la política | 1419 |
| Información de la política | 1419 |
| Versión de la política | 1419 |
| Documento de política JSON | 1419 |
| Más información | 1429 |

| | |
|--|------|
| AWSBackupServiceRolePolicyForS3Backup | 1429 |
| Uso de la política | 1430 |
| Información de la política | 1430 |
| Versión de la política | 1430 |
| Documento de política JSON | 1430 |
| Más información | 1432 |
| AWSBackupServiceRolePolicyForS3Restore | 1432 |
| Uso de la política | 1432 |
| Información de la política | 1432 |
| Versión de la política | 1433 |
| Documento de política JSON | 1433 |
| Más información | 1434 |
| AWSBatchFullAccess | 1434 |
| Uso de la política | 1435 |
| Información de la política | 1435 |
| Versión de la política | 1435 |
| Documento de política JSON | 1435 |
| Más información | 1437 |
| AWSBatchServiceEventTargetRole | 1437 |
| Uso de la política | 1437 |
| Información de la política | 1437 |
| Versión de la política | 1437 |
| Documento de política JSON | 1437 |
| Más información | 1438 |
| AWSBatchServiceRole | 1438 |
| Uso de la política | 1438 |
| Información de la política | 1438 |
| Versión de la política | 1439 |
| Documento de política JSON | 1439 |
| Más información | 1442 |
| AWSBillingConductorFullAccess | 1442 |
| Uso de la política | 1442 |
| Información de la política | 1442 |
| Versión de la política | 1443 |
| Documento de política JSON | 1443 |
| Más información | 1443 |

| | |
|--|------|
| AWSBillingConductorReadOnlyAccess | 1443 |
| Uso de la política | 1444 |
| Información de la política | 1444 |
| Versión de la política | 1444 |
| Documento de política JSON | 1444 |
| Más información | 1445 |
| AWSBillingReadOnlyAccess | 1445 |
| Uso de la política | 1445 |
| Información de la política | 1445 |
| Versión de la política | 1445 |
| Documento de política JSON | 1445 |
| Más información | 1447 |
| AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM | 1447 |
| Uso de la política | 1447 |
| Información de la política | 1447 |
| Versión de la política | 1448 |
| Documento de política JSON | 1448 |
| Más información | 1449 |
| AWSBudgetsActionsWithAWSResourceControlAccess | 1449 |
| Uso de la política | 1449 |
| Información de la política | 1449 |
| Versión de la política | 1450 |
| Documento de política JSON | 1450 |
| Más información | 1451 |
| AWSBudgetsReadOnlyAccess | 1451 |
| Uso de la política | 1451 |
| Información de la política | 1451 |
| Versión de la política | 1452 |
| Documento de política JSON | 1452 |
| Más información | 1452 |
| AWSBugBustFullAccess | 1453 |
| Uso de la política | 1453 |
| Información de la política | 1453 |
| Versión de la política | 1453 |
| Documento de política JSON | 1453 |
| Más información | 1454 |

| | |
|--|------|
| AWSBugBustPlayerAccess | 1455 |
| Uso de la política | 1455 |
| Información de la política | 1455 |
| Versión de la política | 1455 |
| Documento de política JSON | 1455 |
| Más información | 1456 |
| AWSBugBustServiceRolePolicy | 1456 |
| Uso de la política | 1457 |
| Información de la política | 1457 |
| Versión de la política | 1457 |
| Documento de política JSON | 1457 |
| Más información | 1458 |
| AWSCertificateManagerFullAccess | 1458 |
| Uso de la política | 1458 |
| Información de la política | 1458 |
| Versión de la política | 1458 |
| Documento de política JSON | 1458 |
| Más información | 1459 |
| AWSCertificateManagerPrivateCAAuditor | 1460 |
| Uso de la política | 1460 |
| Información de la política | 1460 |
| Versión de la política | 1460 |
| Documento de política JSON | 1460 |
| Más información | 1461 |
| AWSCertificateManagerPrivateCAFullAccess | 1461 |
| Uso de la política | 1461 |
| Información de la política | 1461 |
| Versión de la política | 1462 |
| Documento de política JSON | 1462 |
| Más información | 1462 |
| AWSCertificateManagerPrivateCAPrivilegedUser | 1462 |
| Uso de la política | 1463 |
| Información de la política | 1463 |
| Versión de la política | 1463 |
| Documento de política JSON | 1463 |
| Más información | 1464 |

| | |
|--|------|
| AWSCertificateManagerPrivateCAReadOnly | 1465 |
| Uso de la política | 1465 |
| Información de la política | 1465 |
| Versión de la política | 1465 |
| Documento de política JSON | 1465 |
| Más información | 1466 |
| AWSCertificateManagerPrivateCAUser | 1466 |
| Uso de la política | 1466 |
| Información de la política | 1466 |
| Versión de la política | 1466 |
| Documento de política JSON | 1467 |
| Más información | 1468 |
| AWSCertificateManagerReadOnly | 1468 |
| Uso de la política | 1468 |
| Información de la política | 1468 |
| Versión de la política | 1469 |
| Documento de política JSON | 1469 |
| Más información | 1469 |
| AWSChatbotServiceLinkedRolePolicy | 1469 |
| Uso de la política | 1470 |
| Información de la política | 1470 |
| Versión de la política | 1470 |
| Documento de política JSON | 1470 |
| Más información | 1471 |
| AWSCleanRoomsFullAccess | 1471 |
| Uso de la política | 1471 |
| Información de la política | 1471 |
| Versión de la política | 1471 |
| Documento de política JSON | 1472 |
| Más información | 1476 |
| AWSCleanRoomsFullAccessNoQuerying | 1476 |
| Uso de la política | 1476 |
| Información de la política | 1477 |
| Versión de la política | 1477 |
| Documento de política JSON | 1477 |
| Más información | 1482 |

| | |
|-------------------------------------|------|
| AWSCleanRoomsMLFullAccess | 1482 |
| Uso de la política | 1482 |
| Información de la política | 1482 |
| Versión de la política | 1482 |
| Documento de política JSON | 1483 |
| Más información | 1486 |
| AWSCleanRoomsMLReadOnlyAccess | 1486 |
| Uso de la política | 1487 |
| Información de la política | 1487 |
| Versión de la política | 1487 |
| Documento de política JSON | 1487 |
| Más información | 1488 |
| AWSCleanRoomsReadOnlyAccess | 1488 |
| Uso de la política | 1488 |
| Información de la política | 1488 |
| Versión de la política | 1489 |
| Documento de política JSON | 1489 |
| Más información | 1490 |
| AWSCloud9Administrator | 1490 |
| Uso de la política | 1490 |
| Información de la política | 1491 |
| Versión de la política | 1491 |
| Documento de política JSON | 1491 |
| Más información | 1492 |
| AWSCloud9EnvironmentMember | 1493 |
| Uso de la política | 1493 |
| Información de la política | 1493 |
| Versión de la política | 1493 |
| Documento de política JSON | 1493 |
| Más información | 1495 |
| AWSCloud9ServiceRolePolicy | 1495 |
| Uso de la política | 1495 |
| Información de la política | 1495 |
| Versión de la política | 1495 |
| Documento de política JSON | 1495 |
| Más información | 1498 |

| | |
|---------------------------------------|------|
| AWSCloud9SSMInstanceProfile | 1498 |
| Uso de la política | 1498 |
| Información de la política | 1498 |
| Versión de la política | 1498 |
| Documento de política JSON | 1499 |
| Más información | 1499 |
| AWSCloud9User | 1499 |
| Uso de la política | 1500 |
| Información de la política | 1500 |
| Versión de la política | 1500 |
| Documento de política JSON | 1500 |
| Más información | 1502 |
| AWSCloudFormationFullAccess | 1503 |
| Uso de la política | 1503 |
| Información de la política | 1503 |
| Versión de la política | 1503 |
| Documento de política JSON | 1503 |
| Más información | 1504 |
| AWSCloudFormationReadOnlyAccess | 1504 |
| Uso de la política | 1504 |
| Información de la política | 1504 |
| Versión de la política | 1504 |
| Documento de política JSON | 1505 |
| Más información | 1505 |
| AWSCloudFrontLogger | 1505 |
| Uso de la política | 1505 |
| Información de la política | 1506 |
| Versión de la política | 1506 |
| Documento de política JSON | 1506 |
| Más información | 1506 |
| AWSCloudHSMFullAccess | 1507 |
| Uso de la política | 1507 |
| Información de la política | 1507 |
| Versión de la política | 1507 |
| Documento de política JSON | 1507 |
| Más información | 1508 |

| | |
|---|------|
| AWSCloudHSMReadOnlyAccess | 1508 |
| Uso de la política | 1508 |
| Información de la política | 1508 |
| Versión de la política | 1508 |
| Documento de política JSON | 1508 |
| Más información | 1509 |
| AWSCloudHSMRole | 1509 |
| Uso de la política | 1509 |
| Información de la política | 1509 |
| Versión de la política | 1510 |
| Documento de política JSON | 1510 |
| Más información | 1510 |
| AWSCloudMapDiscoverInstanceAccess | 1511 |
| Uso de la política | 1511 |
| Información de la política | 1511 |
| Versión de la política | 1511 |
| Documento de política JSON | 1511 |
| Más información | 1512 |
| AWSCloudMapFullAccess | 1512 |
| Uso de la política | 1512 |
| Información de la política | 1512 |
| Versión de la política | 1512 |
| Documento de política JSON | 1513 |
| Más información | 1513 |
| AWSCloudMapReadOnlyAccess | 1514 |
| Uso de la política | 1514 |
| Información de la política | 1514 |
| Versión de la política | 1514 |
| Documento de política JSON | 1514 |
| Más información | 1515 |
| AWSCloudMapRegisterInstanceAccess | 1515 |
| Uso de la política | 1515 |
| Información de la política | 1515 |
| Versión de la política | 1515 |
| Documento de política JSON | 1516 |
| Más información | 1516 |

| | |
|---|------|
| AWSCloudShellFullAccess | 1517 |
| Uso de la política | 1517 |
| Información de la política | 1517 |
| Versión de la política | 1517 |
| Documento de política JSON | 1517 |
| Más información | 1518 |
| AWSCloudTrail_FullAccess | 1518 |
| Uso de la política | 1518 |
| Información de la política | 1518 |
| Versión de la política | 1518 |
| Documento de política JSON | 1518 |
| Más información | 1521 |
| AWSCloudTrail_ReadOnlyAccess | 1521 |
| Uso de la política | 1521 |
| Información de la política | 1521 |
| Versión de la política | 1522 |
| Documento de política JSON | 1522 |
| Más información | 1522 |
| AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy | 1523 |
| Uso de la política | 1523 |
| Información de la política | 1523 |
| Versión de la política | 1523 |
| Documento de política JSON | 1523 |
| Más información | 1524 |
| AWSCodeArtifactAdminAccess | 1524 |
| Uso de la política | 1524 |
| Información de la política | 1524 |
| Versión de la política | 1524 |
| Documento de política JSON | 1524 |
| Más información | 1525 |
| AWSCodeArtifactReadOnlyAccess | 1525 |
| Uso de la política | 1525 |
| Información de la política | 1526 |
| Versión de la política | 1526 |
| Documento de política JSON | 1526 |
| Más información | 1527 |

| | |
|-----------------------------------|------|
| AWSCodeBuildAdminAccess | 1527 |
| Uso de la política | 1527 |
| Información de la política | 1527 |
| Versión de la política | 1527 |
| Documento de política JSON | 1528 |
| Más información | 1531 |
| AWSCodeBuildDeveloperAccess | 1531 |
| Uso de la política | 1531 |
| Información de la política | 1531 |
| Versión de la política | 1532 |
| Documento de política JSON | 1532 |
| Más información | 1534 |
| AWSCodeBuildReadOnlyAccess | 1535 |
| Uso de la política | 1535 |
| Información de la política | 1535 |
| Versión de la política | 1535 |
| Documento de política JSON | 1535 |
| Más información | 1537 |
| AWSCodeCommitFullAccess | 1537 |
| Uso de la política | 1537 |
| Información de la política | 1537 |
| Versión de la política | 1537 |
| Documento de política JSON | 1537 |
| Más información | 1542 |
| AWSCodeCommitPowerUser | 1542 |
| Uso de la política | 1542 |
| Información de la política | 1542 |
| Versión de la política | 1543 |
| Documento de política JSON | 1543 |
| Más información | 1548 |
| AWSCodeCommitReadOnly | 1548 |
| Uso de la política | 1548 |
| Información de la política | 1548 |
| Versión de la política | 1548 |
| Documento de política JSON | 1549 |
| Más información | 1551 |

| | |
|--|------|
| AWSCodeDeployDeployerAccess | 1551 |
| Uso de la política | 1551 |
| Información de la política | 1552 |
| Versión de la política | 1552 |
| Documento de política JSON | 1552 |
| Más información | 1553 |
| AWSCodeDeployFullAccess | 1554 |
| Uso de la política | 1554 |
| Información de la política | 1554 |
| Versión de la política | 1554 |
| Documento de política JSON | 1554 |
| Más información | 1556 |
| AWSCodeDeployReadOnlyAccess | 1556 |
| Uso de la política | 1556 |
| Información de la política | 1556 |
| Versión de la política | 1557 |
| Documento de política JSON | 1557 |
| Más información | 1558 |
| AWSCodeDeployRole | 1558 |
| Uso de la política | 1558 |
| Información de la política | 1558 |
| Versión de la política | 1558 |
| Documento de política JSON | 1559 |
| Más información | 1560 |
| AWSCodeDeployRoleForCloudFormation | 1560 |
| Uso de la política | 1560 |
| Información de la política | 1560 |
| Versión de la política | 1561 |
| Documento de política JSON | 1561 |
| Más información | 1561 |
| AWSCodeDeployRoleForECS | 1562 |
| Uso de la política | 1562 |
| Información de la política | 1562 |
| Versión de la política | 1562 |
| Documento de política JSON | 1562 |
| Más información | 1563 |

| | |
|---|------|
| AWSCodeDeployRoleForECSLimited | 1564 |
| Uso de la política | 1564 |
| Información de la política | 1564 |
| Versión de la política | 1564 |
| Documento de política JSON | 1564 |
| Más información | 1566 |
| AWSCodeDeployRoleForLambda | 1566 |
| Uso de la política | 1566 |
| Información de la política | 1566 |
| Versión de la política | 1567 |
| Documento de política JSON | 1567 |
| Más información | 1568 |
| AWSCodeDeployRoleForLambdaLimited | 1568 |
| Uso de la política | 1568 |
| Información de la política | 1568 |
| Versión de la política | 1569 |
| Documento de política JSON | 1569 |
| Más información | 1570 |
| AWSCodePipeline_FullAccess | 1570 |
| Uso de la política | 1570 |
| Información de la política | 1570 |
| Versión de la política | 1571 |
| Documento de política JSON | 1571 |
| Más información | 1575 |
| AWSCodePipeline_ReadOnlyAccess | 1575 |
| Uso de la política | 1575 |
| Información de la política | 1575 |
| Versión de la política | 1575 |
| Documento de política JSON | 1575 |
| Más información | 1577 |
| AWSCodePipelineApproverAccess | 1577 |
| Uso de la política | 1577 |
| Información de la política | 1577 |
| Versión de la política | 1577 |
| Documento de política JSON | 1577 |
| Más información | 1578 |

| | |
|---|------|
| AWSCodePipelineCustomActionAccess | 1578 |
| Uso de la política | 1578 |
| Información de la política | 1578 |
| Versión de la política | 1579 |
| Documento de política JSON | 1579 |
| Más información | 1579 |
| AWSCodeStarFullAccess | 1580 |
| Uso de la política | 1580 |
| Información de la política | 1580 |
| Versión de la política | 1580 |
| Documento de política JSON | 1580 |
| Más información | 1581 |
| AWSCodeStarNotificationsServiceRolePolicy | 1581 |
| Uso de la política | 1581 |
| Información de la política | 1582 |
| Versión de la política | 1582 |
| Documento de política JSON | 1582 |
| Más información | 1583 |
| AWSCodeStarServiceRole | 1583 |
| Uso de la política | 1583 |
| Información de la política | 1584 |
| Versión de la política | 1584 |
| Documento de política JSON | 1584 |
| Más información | 1589 |
| AWSCompromisedKeyQuarantine | 1589 |
| Uso de la política | 1589 |
| Información de la política | 1589 |
| Versión de la política | 1589 |
| Documento de política JSON | 1590 |
| Más información | 1591 |
| AWSCompromisedKeyQuarantineV2 | 1591 |
| Uso de la política | 1591 |
| Información de la política | 1591 |
| Versión de la política | 1591 |
| Documento de política JSON | 1592 |
| Más información | 1593 |

| | |
|---|------|
| AWSConfigMultiAccountSetupPolicy | 1594 |
| Uso de la política | 1594 |
| Información de la política | 1594 |
| Versión de la política | 1594 |
| Documento de política JSON | 1594 |
| Más información | 1596 |
| AWSConfigRemediationServiceRolePolicy | 1596 |
| Uso de la política | 1597 |
| Información de la política | 1597 |
| Versión de la política | 1597 |
| Documento de política JSON | 1597 |
| Más información | 1598 |
| AWSConfigRoleForOrganizations | 1598 |
| Uso de la política | 1598 |
| Información de la política | 1598 |
| Versión de la política | 1598 |
| Documento de política JSON | 1599 |
| Más información | 1599 |
| AWSConfigRulesExecutionRole | 1599 |
| Uso de la política | 1599 |
| Información de la política | 1600 |
| Versión de la política | 1600 |
| Documento de política JSON | 1600 |
| Más información | 1601 |
| AWSConfigServiceRolePolicy | 1601 |
| Uso de la política | 1601 |
| Información de la política | 1601 |
| Versión de la política | 1601 |
| Documento de política JSON | 1602 |
| Más información | 1633 |
| AWSConfigUserAccess | 1633 |
| Uso de la política | 1633 |
| Información de la política | 1633 |
| Versión de la política | 1634 |
| Documento de política JSON | 1634 |
| Más información | 1634 |

| | |
|---|------|
| AWSConnecter | 1635 |
| Uso de la política | 1635 |
| Información de la política | 1635 |
| Versión de la política | 1635 |
| Documento de política JSON | 1635 |
| Más información | 1637 |
| AWSControlTowerAccountServiceRolePolicy | 1638 |
| Uso de la política | 1638 |
| Información de la política | 1638 |
| Versión de la política | 1638 |
| Documento de política JSON | 1638 |
| Más información | 1640 |
| AWSControlTowerServiceRolePolicy | 1640 |
| Uso de la política | 1640 |
| Información de la política | 1640 |
| Versión de la política | 1641 |
| Documento de política JSON | 1641 |
| Más información | 1645 |
| AWSCostAndUsageReportAutomationPolicy | 1645 |
| Uso de la política | 1646 |
| Información de la política | 1646 |
| Versión de la política | 1646 |
| Documento de política JSON | 1646 |
| Más información | 1647 |
| AWSDataExchangeFullAccess | 1647 |
| Uso de la política | 1648 |
| Información de la política | 1648 |
| Versión de la política | 1648 |
| Documento de política JSON | 1648 |
| Más información | 1651 |
| AWSDataExchangeProviderFullAccess | 1651 |
| Uso de la política | 1652 |
| Información de la política | 1652 |
| Versión de la política | 1652 |
| Documento de política JSON | 1652 |
| Más información | 1656 |

| | |
|--|------|
| AWSDataExchangeReadOnly | 1656 |
| Uso de la política | 1656 |
| Información de la política | 1656 |
| Versión de la política | 1656 |
| Documento de política JSON | 1657 |
| Más información | 1657 |
| AWSDataExchangeSubscriberFullAccess | 1658 |
| Uso de la política | 1658 |
| Información de la política | 1658 |
| Versión de la política | 1658 |
| Documento de política JSON | 1658 |
| Más información | 1660 |
| AWSDataLifecycleManagerServiceRole | 1661 |
| Uso de la política | 1661 |
| Información de la política | 1661 |
| Versión de la política | 1661 |
| Documento de política JSON | 1661 |
| Más información | 1662 |
| AWSDataLifecycleManagerServiceRoleForAMIManagement | 1663 |
| Uso de la política | 1663 |
| Información de la política | 1663 |
| Versión de la política | 1663 |
| Documento de política JSON | 1663 |
| Más información | 1665 |
| AWSDataLifecycleManagerSSMFullAccess | 1665 |
| Uso de la política | 1665 |
| Información de la política | 1665 |
| Versión de la política | 1665 |
| Documento de política JSON | 1666 |
| Más información | 1667 |
| AWSDataPipeline_FullAccess | 1667 |
| Uso de la política | 1667 |
| Información de la política | 1667 |
| Versión de la política | 1668 |
| Documento de política JSON | 1668 |
| Más información | 1669 |

| | |
|---|------|
| AWSDatapipeline_PowerUser | 1669 |
| Uso de la política | 1669 |
| Información de la política | 1669 |
| Versión de la política | 1669 |
| Documento de política JSON | 1670 |
| Más información | 1671 |
| AWSDatasyncDiscoveryServiceRolePolicy | 1671 |
| Uso de la política | 1671 |
| Información de la política | 1671 |
| Versión de la política | 1671 |
| Documento de política JSON | 1672 |
| Más información | 1673 |
| AWSDatasyncFullAccess | 1673 |
| Uso de la política | 1673 |
| Información de la política | 1673 |
| Versión de la política | 1673 |
| Documento de política JSON | 1673 |
| Más información | 1675 |
| AWSDatasyncReadOnlyAccess | 1675 |
| Uso de la política | 1675 |
| Información de la política | 1675 |
| Versión de la política | 1675 |
| Documento de política JSON | 1676 |
| Más información | 1676 |
| AWSDeepLensLambdaFunctionAccessPolicy | 1677 |
| Uso de la política | 1677 |
| Información de la política | 1677 |
| Versión de la política | 1677 |
| Documento de política JSON | 1677 |
| Más información | 1678 |
| AWSDeepLensServiceRolePolicy | 1679 |
| Uso de la política | 1679 |
| Información de la política | 1679 |
| Versión de la política | 1679 |
| Documento de política JSON | 1679 |
| Más información | 1686 |

| | |
|--|------|
| AWSDeeperRacerAccountAdminAccess | 1687 |
| Uso de la política | 1687 |
| Información de la política | 1687 |
| Versión de la política | 1687 |
| Documento de política JSON | 1687 |
| Más información | 1688 |
| AWSDeeperRacerCloudFormationAccessPolicy | 1688 |
| Uso de la política | 1688 |
| Información de la política | 1688 |
| Versión de la política | 1689 |
| Documento de política JSON | 1689 |
| Más información | 1692 |
| AWSDeeperRacerDefaultMultiUserAccess | 1692 |
| Uso de la política | 1692 |
| Información de la política | 1692 |
| Versión de la política | 1692 |
| Documento de política JSON | 1693 |
| Más información | 1694 |
| AWSDeeperRacerFullAccess | 1694 |
| Uso de la política | 1694 |
| Información de la política | 1695 |
| Versión de la política | 1695 |
| Documento de política JSON | 1695 |
| Más información | 1696 |
| AWSDeeperRacerRoboMakerAccessPolicy | 1696 |
| Uso de la política | 1696 |
| Información de la política | 1696 |
| Versión de la política | 1697 |
| Documento de política JSON | 1697 |
| Más información | 1699 |
| AWSDeeperRacerServiceRolePolicy | 1699 |
| Uso de la política | 1699 |
| Información de la política | 1699 |
| Versión de la política | 1699 |
| Documento de política JSON | 1700 |
| Más información | 1703 |

| | |
|--|------|
| AWSDenyAll | 1703 |
| Uso de la política | 1703 |
| Información de la política | 1703 |
| Versión de la política | 1703 |
| Documento de política JSON | 1704 |
| Más información | 1704 |
| AWSDeviceFarmFullAccess | 1704 |
| Uso de la política | 1704 |
| Información de la política | 1705 |
| Versión de la política | 1705 |
| Documento de política JSON | 1705 |
| Más información | 1705 |
| AWSDeviceFarmServiceRolePolicy | 1706 |
| Uso de la política | 1706 |
| Información de la política | 1706 |
| Versión de la política | 1706 |
| Documento de política JSON | 1706 |
| Más información | 1708 |
| AWSDeviceFarmTestGridServiceRolePolicy | 1709 |
| Uso de la política | 1709 |
| Información de la política | 1709 |
| Versión de la política | 1709 |
| Documento de política JSON | 1709 |
| Más información | 1711 |
| AWSDirectConnectFullAccess | 1712 |
| Uso de la política | 1712 |
| Información de la política | 1712 |
| Versión de la política | 1712 |
| Documento de política JSON | 1712 |
| Más información | 1713 |
| AWSDirectConnectReadOnlyAccess | 1713 |
| Uso de la política | 1713 |
| Información de la política | 1713 |
| Versión de la política | 1713 |
| Documento de política JSON | 1714 |
| Más información | 1714 |

| | |
|--|------|
| AWSDirectConnectServiceRolePolicy | 1714 |
| Uso de la política | 1714 |
| Información de la política | 1715 |
| Versión de la política | 1715 |
| Documento de política JSON | 1715 |
| Más información | 1715 |
| AWSDirectoryServiceFullAccess | 1716 |
| Uso de la política | 1716 |
| Información de la política | 1716 |
| Versión de la política | 1716 |
| Documento de política JSON | 1716 |
| Más información | 1718 |
| AWSDirectoryServiceReadOnlyAccess | 1718 |
| Uso de la política | 1718 |
| Información de la política | 1718 |
| Versión de la política | 1719 |
| Documento de política JSON | 1719 |
| Más información | 1720 |
| AWSDiscoveryContinuousExportFirehosePolicy | 1720 |
| Uso de la política | 1720 |
| Información de la política | 1720 |
| Versión de la política | 1720 |
| Documento de política JSON | 1721 |
| Más información | 1722 |
| AWSDMSFleetAdvisorServiceRolePolicy | 1722 |
| Uso de la política | 1722 |
| Información de la política | 1722 |
| Versión de la política | 1722 |
| Documento de política JSON | 1723 |
| Más información | 1723 |
| AWSDMSServerlessServiceRolePolicy | 1723 |
| Uso de la política | 1723 |
| Información de la política | 1723 |
| Versión de la política | 1724 |
| Documento de política JSON | 1724 |
| Más información | 1725 |

| | |
|---|------|
| AWSEC2CapacityReservationFleetRolePolicy | 1725 |
| Uso de la política | 1726 |
| Información de la política | 1726 |
| Versión de la política | 1726 |
| Documento de política JSON | 1726 |
| Más información | 1727 |
| AWSEC2FleetServiceRolePolicy | 1727 |
| Uso de la política | 1728 |
| Información de la política | 1728 |
| Versión de la política | 1728 |
| Documento de política JSON | 1728 |
| Más información | 1730 |
| AWSEC2SpotFleetServiceRolePolicy | 1730 |
| Uso de la política | 1730 |
| Información de la política | 1731 |
| Versión de la política | 1731 |
| Documento de política JSON | 1731 |
| Más información | 1733 |
| AWSEC2SpotServiceRolePolicy | 1733 |
| Uso de la política | 1733 |
| Información de la política | 1733 |
| Versión de la política | 1733 |
| Documento de política JSON | 1734 |
| Más información | 1735 |
| AWSECRPullThroughCache_ServiceRolePolicy | 1735 |
| Uso de la política | 1735 |
| Información de la política | 1736 |
| Versión de la política | 1736 |
| Documento de política JSON | 1736 |
| Más información | 1737 |
| AWSElasticBeanstalkCustomPlatformforEC2Role | 1737 |
| Uso de la política | 1737 |
| Información de la política | 1737 |
| Versión de la política | 1737 |
| Documento de política JSON | 1738 |
| Más información | 1739 |

| | |
|---|------|
| AWSElasticBeanstalkEnhancedHealth | 1740 |
| Uso de la política | 1740 |
| Información de la política | 1740 |
| Versión de la política | 1740 |
| Documento de política JSON | 1740 |
| Más información | 1741 |
| AWSElasticBeanstalkMaintenance | 1741 |
| Uso de la política | 1742 |
| Información de la política | 1742 |
| Versión de la política | 1742 |
| Documento de política JSON | 1742 |
| Más información | 1743 |
| AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy | 1743 |
| Uso de la política | 1743 |
| Información de la política | 1743 |
| Versión de la política | 1744 |
| Documento de política JSON | 1744 |
| Más información | 1750 |
| AWSElasticBeanstalkManagedUpdatesServiceRolePolicy | 1751 |
| Uso de la política | 1751 |
| Información de la política | 1751 |
| Versión de la política | 1751 |
| Documento de política JSON | 1751 |
| Más información | 1757 |
| AWSElasticBeanstalkMulticontainerDocker | 1757 |
| Uso de la política | 1757 |
| Información de la política | 1757 |
| Versión de la política | 1757 |
| Documento de política JSON | 1757 |
| Más información | 1758 |
| AWSElasticBeanstalkReadOnly | 1759 |
| Uso de la política | 1759 |
| Información de la política | 1759 |
| Versión de la política | 1759 |
| Documento de política JSON | 1759 |
| Más información | 1761 |

| | |
|---|------|
| AWSElasticBeanstalkRoleCore | 1762 |
| Uso de la política | 1762 |
| Información de la política | 1762 |
| Versión de la política | 1762 |
| Documento de política JSON | 1762 |
| Más información | 1767 |
| AWSElasticBeanstalkRoleCWL | 1767 |
| Uso de la política | 1768 |
| Información de la política | 1768 |
| Versión de la política | 1768 |
| Documento de política JSON | 1768 |
| Más información | 1769 |
| AWSElasticBeanstalkRoleECS | 1769 |
| Uso de la política | 1769 |
| Información de la política | 1769 |
| Versión de la política | 1769 |
| Documento de política JSON | 1769 |
| Más información | 1770 |
| AWSElasticBeanstalkRoleRDS | 1771 |
| Uso de la política | 1771 |
| Información de la política | 1771 |
| Versión de la política | 1771 |
| Documento de política JSON | 1771 |
| Más información | 1772 |
| AWSElasticBeanstalkRoleSNS | 1772 |
| Uso de la política | 1772 |
| Información de la política | 1772 |
| Versión de la política | 1773 |
| Documento de política JSON | 1773 |
| Más información | 1774 |
| AWSElasticBeanstalkRoleWorkerTier | 1774 |
| Uso de la política | 1774 |
| Información de la política | 1774 |
| Versión de la política | 1774 |
| Documento de política JSON | 1775 |
| Más información | 1775 |

| | |
|---|------|
| AWSElasticBeanstalkService | 1776 |
| Uso de la política | 1776 |
| Información de la política | 1776 |
| Versión de la política | 1776 |
| Documento de política JSON | 1776 |
| Más información | 1781 |
| AWSElasticBeanstalkServiceRolePolicy | 1781 |
| Uso de la política | 1781 |
| Información de la política | 1781 |
| Versión de la política | 1781 |
| Documento de política JSON | 1782 |
| Más información | 1783 |
| AWSElasticBeanstalkWebTier | 1783 |
| Uso de la política | 1783 |
| Información de la política | 1783 |
| Versión de la política | 1784 |
| Documento de política JSON | 1784 |
| Más información | 1785 |
| AWSElasticBeanstalkWorkerTier | 1785 |
| Uso de la política | 1786 |
| Información de la política | 1786 |
| Versión de la política | 1786 |
| Documento de política JSON | 1786 |
| Más información | 1788 |
| AWSElasticDisasterRecoveryAgentInstallationPolicy | 1788 |
| Uso de la política | 1789 |
| Información de la política | 1789 |
| Versión de la política | 1789 |
| Documento de política JSON | 1789 |
| Más información | 1791 |
| AWSElasticDisasterRecoveryAgentPolicy | 1791 |
| Uso de la política | 1791 |
| Información de la política | 1791 |
| Versión de la política | 1791 |
| Documento de política JSON | 1792 |
| Más información | 1792 |

| | |
|---|------|
| AWSElasticDisasterRecoveryConsoleFullAccess | 1793 |
| Uso de la política | 1793 |
| Información de la política | 1793 |
| Versión de la política | 1793 |
| Documento de política JSON | 1793 |
| Más información | 1803 |
| AWSElasticDisasterRecoveryConsoleFullAccess_v2 | 1803 |
| Uso de la política | 1804 |
| Información de la política | 1804 |
| Versión de la política | 1804 |
| Documento de política JSON | 1804 |
| Más información | 1817 |
| AWSElasticDisasterRecoveryConversionServerPolicy | 1817 |
| Uso de la política | 1817 |
| Información de la política | 1817 |
| Versión de la política | 1818 |
| Documento de política JSON | 1818 |
| Más información | 1818 |
| AWSElasticDisasterRecoveryCrossAccountReplicationPolicy | 1819 |
| Uso de la política | 1819 |
| Información de la política | 1819 |
| Versión de la política | 1819 |
| Documento de política JSON | 1819 |
| Más información | 1820 |
| AWSElasticDisasterRecoveryEc2InstancePolicy | 1821 |
| Uso de la política | 1821 |
| Información de la política | 1821 |
| Versión de la política | 1821 |
| Documento de política JSON | 1821 |
| Más información | 1823 |
| AWSElasticDisasterRecoveryFailbackInstallationPolicy | 1824 |
| Uso de la política | 1824 |
| Información de la política | 1824 |
| Versión de la política | 1824 |
| Documento de política JSON | 1824 |
| Más información | 1825 |

| | |
|--|------|
| AWSElasticDisasterRecoveryFailbackPolicy | 1825 |
| Uso de la política | 1826 |
| Información de la política | 1826 |
| Versión de la política | 1826 |
| Documento de política JSON | 1826 |
| Más información | 1827 |
| AWSElasticDisasterRecoveryLaunchActionsPolicy | 1828 |
| Uso de la política | 1828 |
| Información de la política | 1828 |
| Versión de la política | 1828 |
| Documento de política JSON | 1828 |
| Más información | 1834 |
| AWSElasticDisasterRecoveryNetworkReplicationPolicy | 1835 |
| Uso de la política | 1835 |
| Información de la política | 1835 |
| Versión de la política | 1835 |
| Documento de política JSON | 1835 |
| Más información | 1836 |
| AWSElasticDisasterRecoveryReadOnlyAccess | 1836 |
| Uso de la política | 1836 |
| Información de la política | 1837 |
| Versión de la política | 1837 |
| Documento de política JSON | 1837 |
| Más información | 1839 |
| AWSElasticDisasterRecoveryRecoveryInstancePolicy | 1839 |
| Uso de la política | 1840 |
| Información de la política | 1840 |
| Versión de la política | 1840 |
| Documento de política JSON | 1840 |
| Más información | 1843 |
| AWSElasticDisasterRecoveryReplicationServerPolicy | 1843 |
| Uso de la política | 1843 |
| Información de la política | 1843 |
| Versión de la política | 1844 |
| Documento de política JSON | 1844 |
| Más información | 1846 |

| | |
|---|------|
| AWSElasticDisasterRecoveryServiceRolePolicy | 1846 |
| Uso de la política | 1846 |
| Información de la política | 1846 |
| Versión de la política | 1847 |
| Documento de política JSON | 1847 |
| Más información | 1855 |
| AWSElasticDisasterRecoveryStagingAccountPolicy | 1855 |
| Uso de la política | 1856 |
| Información de la política | 1856 |
| Versión de la política | 1856 |
| Documento de política JSON | 1856 |
| Más información | 1857 |
| AWSElasticDisasterRecoveryStagingAccountPolicy_v2 | 1857 |
| Uso de la política | 1858 |
| Información de la política | 1858 |
| Versión de la política | 1858 |
| Documento de política JSON | 1858 |
| Más información | 1859 |
| AWSElasticLoadBalancingClassicServiceRolePolicy | 1859 |
| Uso de la política | 1860 |
| Información de la política | 1860 |
| Versión de la política | 1860 |
| Documento de política JSON | 1860 |
| Más información | 1861 |
| AWSElasticLoadBalancingServiceRolePolicy | 1861 |
| Uso de la política | 1861 |
| Información de la política | 1861 |
| Versión de la política | 1862 |
| Documento de política JSON | 1862 |
| Más información | 1863 |
| AWSElementalMediaConvertFullAccess | 1863 |
| Uso de la política | 1863 |
| Información de la política | 1863 |
| Versión de la política | 1864 |
| Documento de política JSON | 1864 |
| Más información | 1865 |

| | |
|--|------|
| AWSElementalMediaConvertReadOnly | 1865 |
| Uso de la política | 1865 |
| Información de la política | 1865 |
| Versión de la política | 1865 |
| Documento de política JSON | 1865 |
| Más información | 1866 |
| AWSElementalMediaLiveFullAccess | 1866 |
| Uso de la política | 1866 |
| Información de la política | 1866 |
| Versión de la política | 1867 |
| Documento de política JSON | 1867 |
| Más información | 1867 |
| AWSElementalMediaLiveReadOnly | 1867 |
| Uso de la política | 1867 |
| Información de la política | 1868 |
| Versión de la política | 1868 |
| Documento de política JSON | 1868 |
| Más información | 1868 |
| AWSElementalMediaPackageFullAccess | 1869 |
| Uso de la política | 1869 |
| Información de la política | 1869 |
| Versión de la política | 1869 |
| Documento de política JSON | 1869 |
| Más información | 1869 |
| AWSElementalMediaPackageReadOnly | 1870 |
| Uso de la política | 1870 |
| Información de la política | 1870 |
| Versión de la política | 1870 |
| Documento de política JSON | 1870 |
| Más información | 1871 |
| AWSElementalMediaPackageV2FullAccess | 1871 |
| Uso de la política | 1871 |
| Información de la política | 1871 |
| Versión de la política | 1871 |
| Documento de política JSON | 1872 |
| Más información | 1872 |

| | |
|---|------|
| AWSElementalMediaPackageV2ReadOnly | 1872 |
| Uso de la política | 1872 |
| Información de la política | 1872 |
| Versión de la política | 1873 |
| Documento de política JSON | 1873 |
| Más información | 1873 |
| AWSElementalMediaStoreFullAccess | 1873 |
| Uso de la política | 1874 |
| Información de la política | 1874 |
| Versión de la política | 1874 |
| Documento de política JSON | 1874 |
| Más información | 1875 |
| AWSElementalMediaStoreReadOnly | 1875 |
| Uso de la política | 1875 |
| Información de la política | 1875 |
| Versión de la política | 1875 |
| Documento de política JSON | 1875 |
| Más información | 1876 |
| AWSElementalMediaTailorFullAccess | 1876 |
| Uso de la política | 1876 |
| Información de la política | 1876 |
| Versión de la política | 1877 |
| Documento de política JSON | 1877 |
| Más información | 1877 |
| AWSElementalMediaTailorReadOnly | 1877 |
| Uso de la política | 1878 |
| Información de la política | 1878 |
| Versión de la política | 1878 |
| Documento de política JSON | 1878 |
| Más información | 1878 |
| AWSEnhancedClassicNetworkingMangementPolicy | 1879 |
| Uso de la política | 1879 |
| Información de la política | 1879 |
| Versión de la política | 1879 |
| Documento de política JSON | 1879 |
| Más información | 1880 |

| | |
|--|------|
| AWSEntityResolutionConsoleFullAccess | 1880 |
| Uso de la política | 1880 |
| Información de la política | 1880 |
| Versión de la política | 1880 |
| Documento de política JSON | 1881 |
| Más información | 1883 |
| AWSEntityResolutionConsoleReadOnlyAccess | 1884 |
| Uso de la política | 1884 |
| Información de la política | 1884 |
| Versión de la política | 1884 |
| Documento de política JSON | 1884 |
| Más información | 1885 |
| AWSFaultInjectionSimulatorEC2Access | 1885 |
| Uso de la política | 1885 |
| Información de la política | 1885 |
| Versión de la política | 1885 |
| Documento de política JSON | 1886 |
| Más información | 1887 |
| AWSFaultInjectionSimulatorECSAccess | 1887 |
| Uso de la política | 1887 |
| Información de la política | 1888 |
| Versión de la política | 1888 |
| Documento de política JSON | 1888 |
| Más información | 1890 |
| AWSFaultInjectionSimulatorEKSAccess | 1890 |
| Uso de la política | 1890 |
| Información de la política | 1890 |
| Versión de la política | 1890 |
| Documento de política JSON | 1891 |
| Más información | 1892 |
| AWSFaultInjectionSimulatorNetworkAccess | 1892 |
| Uso de la política | 1892 |
| Información de la política | 1892 |
| Versión de la política | 1892 |
| Documento de política JSON | 1893 |
| Más información | 1900 |

| | |
|---|------|
| AWSFaultInjectionSimulatorRDSAccess | 1900 |
| Uso de la política | 1900 |
| Información de la política | 1900 |
| Versión de la política | 1900 |
| Documento de política JSON | 1901 |
| Más información | 1902 |
| AWSFaultInjectionSimulatorSSMAccess | 1902 |
| Uso de la política | 1902 |
| Información de la política | 1902 |
| Versión de la política | 1902 |
| Documento de política JSON | 1903 |
| Más información | 1904 |
| AWSFinSpaceServiceRolePolicy | 1904 |
| Uso de la política | 1904 |
| Información de la política | 1904 |
| Versión de la política | 1905 |
| Documento de política JSON | 1905 |
| Más información | 1905 |
| AWSFMAdminFullAccess | 1905 |
| Uso de la política | 1906 |
| Información de la política | 1906 |
| Versión de la política | 1906 |
| Documento de política JSON | 1906 |
| Más información | 1908 |
| AWSFMAdminReadOnlyAccess | 1908 |
| Uso de la política | 1908 |
| Información de la política | 1908 |
| Versión de la política | 1909 |
| Documento de política JSON | 1909 |
| Más información | 1910 |
| AWSFMMemberReadOnlyAccess | 1911 |
| Uso de la política | 1911 |
| Información de la política | 1911 |
| Versión de la política | 1911 |
| Documento de política JSON | 1911 |
| Más información | 1912 |

| | |
|---|------|
| AWSForWordPressPluginPolicy | 1912 |
| Uso de la política | 1912 |
| Información de la política | 1912 |
| Versión de la política | 1912 |
| Documento de política JSON | 1913 |
| Más información | 1914 |
| AWSGitSyncServiceRolePolicy | 1915 |
| Uso de la política | 1915 |
| Información de la política | 1915 |
| Versión de la política | 1915 |
| Documento de política JSON | 1915 |
| Más información | 1916 |
| AWSGlobalAcceleratorSLRPolicy | 1916 |
| Uso de la política | 1916 |
| Información de la política | 1916 |
| Versión de la política | 1916 |
| Documento de política JSON | 1917 |
| Más información | 1918 |
| AWSGlueConsoleFullAccess | 1918 |
| Uso de la política | 1919 |
| Información de la política | 1919 |
| Versión de la política | 1919 |
| Documento de política JSON | 1919 |
| Más información | 1923 |
| AWSGlueConsoleSageMakerNotebookFullAccess | 1924 |
| Uso de la política | 1924 |
| Información de la política | 1924 |
| Versión de la política | 1924 |
| Documento de política JSON | 1924 |
| Más información | 1929 |
| AwsGlueDataBrewFullAccessPolicy | 1930 |
| Uso de la política | 1930 |
| Información de la política | 1930 |
| Versión de la política | 1930 |
| Documento de política JSON | 1930 |
| Más información | 1935 |

| | |
|--|------|
| AWSGlueDataBrewServiceRole | 1936 |
| Uso de la política | 1936 |
| Información de la política | 1936 |
| Versión de la política | 1936 |
| Documento de política JSON | 1936 |
| Más información | 1939 |
| AWSGlueSchemaRegistryFullAccess | 1939 |
| Uso de la política | 1940 |
| Información de la política | 1940 |
| Versión de la política | 1940 |
| Documento de política JSON | 1940 |
| Más información | 1941 |
| AWSGlueSchemaRegistryReadOnlyAccess | 1942 |
| Uso de la política | 1942 |
| Información de la política | 1942 |
| Versión de la política | 1942 |
| Documento de política JSON | 1942 |
| Más información | 1943 |
| AWSGlueServiceNotebookRole | 1943 |
| Uso de la política | 1943 |
| Información de la política | 1943 |
| Versión de la política | 1944 |
| Documento de política JSON | 1944 |
| Más información | 1946 |
| AWSGlueServiceRole | 1946 |
| Uso de la política | 1946 |
| Información de la política | 1947 |
| Versión de la política | 1947 |
| Documento de política JSON | 1947 |
| Más información | 1949 |
| AwsGlueSessionUserRestrictedNotebookPolicy | 1949 |
| Uso de la política | 1950 |
| Información de la política | 1950 |
| Versión de la política | 1950 |
| Documento de política JSON | 1950 |
| Más información | 1953 |

| | |
|---|------|
| AwsGlueSessionUserRestrictedNotebookServiceRole | 1953 |
| Uso de la política | 1953 |
| Información de la política | 1953 |
| Versión de la política | 1953 |
| Documento de política JSON | 1954 |
| Más información | 1957 |
| AwsGlueSessionUserRestrictedPolicy | 1958 |
| Uso de la política | 1958 |
| Información de la política | 1958 |
| Versión de la política | 1958 |
| Documento de política JSON | 1958 |
| Más información | 1960 |
| AwsGlueSessionUserRestrictedServiceRole | 1961 |
| Uso de la política | 1961 |
| Información de la política | 1961 |
| Versión de la política | 1961 |
| Documento de política JSON | 1961 |
| Más información | 1965 |
| AWSGrafanaAccountAdministrator | 1965 |
| Uso de la política | 1965 |
| Información de la política | 1965 |
| Versión de la política | 1966 |
| Documento de política JSON | 1966 |
| Más información | 1967 |
| AWSGrafanaConsoleReadOnlyAccess | 1967 |
| Uso de la política | 1967 |
| Información de la política | 1967 |
| Versión de la política | 1967 |
| Documento de política JSON | 1968 |
| Más información | 1968 |
| AWSGrafanaWorkspacePermissionManagement | 1968 |
| Uso de la política | 1968 |
| Información de la política | 1969 |
| Versión de la política | 1969 |
| Documento de política JSON | 1969 |
| Más información | 1970 |

| | |
|---|------|
| AWSGrafanaWorkspacePermissionManagementV2 | 1970 |
| Uso de la política | 1970 |
| Información de la política | 1970 |
| Versión de la política | 1971 |
| Documento de política JSON | 1971 |
| Más información | 1972 |
| AWSGreengrassFullAccess | 1972 |
| Uso de la política | 1972 |
| Información de la política | 1972 |
| Versión de la política | 1972 |
| Documento de política JSON | 1973 |
| Más información | 1973 |
| AWSGreengrassReadOnlyAccess | 1973 |
| Uso de la política | 1973 |
| Información de la política | 1973 |
| Versión de la política | 1974 |
| Documento de política JSON | 1974 |
| Más información | 1974 |
| AWSGreengrassResourceAccessRolePolicy | 1975 |
| Uso de la política | 1975 |
| Información de la política | 1975 |
| Versión de la política | 1975 |
| Documento de política JSON | 1975 |
| Más información | 1978 |
| AWSGroundStationAgentInstancePolicy | 1978 |
| Uso de la política | 1978 |
| Información de la política | 1978 |
| Versión de la política | 1978 |
| Documento de política JSON | 1978 |
| Más información | 1979 |
| AWSHealth_EventProcessorServiceRolePolicy | 1979 |
| Uso de la política | 1979 |
| Información de la política | 1979 |
| Versión de la política | 1980 |
| Documento de política JSON | 1980 |
| Más información | 1981 |

| | |
|---|------|
| AWSHealthFullAccess | 1981 |
| Uso de la política | 1981 |
| Información de la política | 1981 |
| Versión de la política | 1981 |
| Documento de política JSON | 1981 |
| Más información | 1982 |
| AWSHealthImagingFullAccess | 1983 |
| Uso de la política | 1983 |
| Información de la política | 1983 |
| Versión de la política | 1983 |
| Documento de política JSON | 1983 |
| Más información | 1984 |
| AWSHealthImagingReadOnlyAccess | 1984 |
| Uso de la política | 1984 |
| Información de la política | 1984 |
| Versión de la política | 1985 |
| Documento de política JSON | 1985 |
| Más información | 1985 |
| AWSIAMIdentityCenterAllowListForIdentityContext | 1986 |
| Uso de la política | 1986 |
| Información de la política | 1986 |
| Versión de la política | 1986 |
| Documento de política JSON | 1986 |
| Más información | 1988 |
| AWSIdentitySyncFullAccess | 1988 |
| Uso de la política | 1988 |
| Información de la política | 1989 |
| Versión de la política | 1989 |
| Documento de política JSON | 1989 |
| Más información | 1990 |
| AWSIdentitySyncReadOnlyAccess | 1990 |
| Uso de la política | 1990 |
| Información de la política | 1990 |
| Versión de la política | 1990 |
| Documento de política JSON | 1991 |
| Más información | 1991 |

| | |
|---|------|
| AWSImageBuilderFullAccess | 1991 |
| Uso de la política | 1991 |
| Información de la política | 1992 |
| Versión de la política | 1992 |
| Documento de política JSON | 1992 |
| Más información | 1995 |
| AWSImageBuilderReadOnlyAccess | 1995 |
| Uso de la política | 1995 |
| Información de la política | 1995 |
| Versión de la política | 1995 |
| Documento de política JSON | 1996 |
| Más información | 1996 |
| AWSImportExportFullAccess | 1996 |
| Uso de la política | 1997 |
| Información de la política | 1997 |
| Versión de la política | 1997 |
| Documento de política JSON | 1997 |
| Más información | 1997 |
| AWSImportExportReadOnlyAccess | 1998 |
| Uso de la política | 1998 |
| Información de la política | 1998 |
| Versión de la política | 1998 |
| Documento de política JSON | 1998 |
| Más información | 1999 |
| AWSIncidentManagerIncidentAccessServiceRolePolicy | 1999 |
| Uso de la política | 1999 |
| Información de la política | 1999 |
| Versión de la política | 1999 |
| Documento de política JSON | 2000 |
| Más información | 2000 |
| AWSIncidentManagerResolverAccess | 2000 |
| Uso de la política | 2001 |
| Información de la política | 2001 |
| Versión de la política | 2001 |
| Documento de política JSON | 2001 |
| Más información | 2002 |

| | |
|---|------|
| AWSIncidentManagerServiceRolePolicy | 2002 |
| Uso de la política | 2003 |
| Información de la política | 2003 |
| Versión de la política | 2003 |
| Documento de política JSON | 2003 |
| Más información | 2004 |
| AWSIoT1ClickFullAccess | 2004 |
| Uso de la política | 2004 |
| Información de la política | 2005 |
| Versión de la política | 2005 |
| Documento de política JSON | 2005 |
| Más información | 2005 |
| AWSIoT1ClickReadOnlyAccess | 2006 |
| Uso de la política | 2006 |
| Información de la política | 2006 |
| Versión de la política | 2006 |
| Documento de política JSON | 2006 |
| Más información | 2007 |
| AWSIoTAnalyticsFullAccess | 2007 |
| Uso de la política | 2007 |
| Información de la política | 2007 |
| Versión de la política | 2007 |
| Documento de política JSON | 2008 |
| Más información | 2008 |
| AWSIoTAnalyticsReadOnlyAccess | 2008 |
| Uso de la política | 2008 |
| Información de la política | 2008 |
| Versión de la política | 2009 |
| Documento de política JSON | 2009 |
| Más información | 2009 |
| AWSIoTConfigAccess | 2010 |
| Uso de la política | 2010 |
| Información de la política | 2010 |
| Versión de la política | 2010 |
| Documento de política JSON | 2010 |
| Más información | 2014 |

| | |
|---|------|
| AWSIoTConfigReadOnlyAccess | 2014 |
| Uso de la política | 2014 |
| Información de la política | 2014 |
| Versión de la política | 2015 |
| Documento de política JSON | 2015 |
| Más información | 2017 |
| AWSIoTDataAccess | 2017 |
| Uso de la política | 2017 |
| Información de la política | 2017 |
| Versión de la política | 2017 |
| Documento de política JSON | 2018 |
| Más información | 2018 |
| AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction | 2018 |
| Uso de la política | 2019 |
| Información de la política | 2019 |
| Versión de la política | 2019 |
| Documento de política JSON | 2019 |
| Más información | 2020 |
| AWSIoTDeviceDefenderAudit | 2020 |
| Uso de la política | 2020 |
| Información de la política | 2020 |
| Versión de la política | 2020 |
| Documento de política JSON | 2021 |
| Más información | 2021 |
| AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction | 2022 |
| Uso de la política | 2022 |
| Información de la política | 2022 |
| Versión de la política | 2022 |
| Documento de política JSON | 2022 |
| Más información | 2023 |
| AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction | 2023 |
| Uso de la política | 2024 |
| Información de la política | 2024 |
| Versión de la política | 2024 |
| Documento de política JSON | 2024 |
| Más información | 2025 |

| | |
|--|------|
| AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction | 2025 |
| Uso de la política | 2025 |
| Información de la política | 2025 |
| Versión de la política | 2025 |
| Documento de política JSON | 2026 |
| Más información | 2026 |
| AWSIoTDeviceDefenderUpdateCACertMitigationAction | 2026 |
| Uso de la política | 2026 |
| Información de la política | 2027 |
| Versión de la política | 2027 |
| Documento de política JSON | 2027 |
| Más información | 2027 |
| AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction | 2028 |
| Uso de la política | 2028 |
| Información de la política | 2028 |
| Versión de la política | 2028 |
| Documento de política JSON | 2028 |
| Más información | 2029 |
| AWSIoTDeviceTesterForFreeRTOSFullAccess | 2029 |
| Uso de la política | 2029 |
| Información de la política | 2029 |
| Versión de la política | 2030 |
| Documento de política JSON | 2030 |
| Más información | 2036 |
| AWSIoTDeviceTesterForGreengrassFullAccess | 2036 |
| Uso de la política | 2036 |
| Información de la política | 2036 |
| Versión de la política | 2037 |
| Documento de política JSON | 2037 |
| Más información | 2040 |
| AWSIoTEventsFullAccess | 2040 |
| Uso de la política | 2040 |
| Información de la política | 2040 |
| Versión de la política | 2040 |
| Documento de política JSON | 2041 |
| Más información | 2041 |

| | |
|--|------|
| AWSIoTEventsReadOnlyAccess | 2041 |
| Uso de la política | 2041 |
| Información de la política | 2041 |
| Versión de la política | 2042 |
| Documento de política JSON | 2042 |
| Más información | 2042 |
| AWSIoTFleetHubFederationAccess | 2043 |
| Uso de la política | 2043 |
| Información de la política | 2043 |
| Versión de la política | 2043 |
| Documento de política JSON | 2043 |
| Más información | 2045 |
| AWSIoTFleetwiseServiceRolePolicy | 2045 |
| Uso de la política | 2045 |
| Información de la política | 2045 |
| Versión de la política | 2046 |
| Documento de política JSON | 2046 |
| Más información | 2046 |
| AWSIoTFullAccess | 2047 |
| Uso de la política | 2047 |
| Información de la política | 2047 |
| Versión de la política | 2047 |
| Documento de política JSON | 2047 |
| Más información | 2048 |
| AWSIoTLogging | 2048 |
| Uso de la política | 2048 |
| Información de la política | 2048 |
| Versión de la política | 2048 |
| Documento de política JSON | 2048 |
| Más información | 2049 |
| AWSIoTOTAUpdate | 2049 |
| Uso de la política | 2049 |
| Información de la política | 2049 |
| Versión de la política | 2050 |
| Documento de política JSON | 2050 |
| Más información | 2050 |

| | |
|---|------|
| AWSIoTRoboRunnerFullAccess | 2051 |
| Uso de la política | 2051 |
| Información de la política | 2051 |
| Versión de la política | 2051 |
| Documento de política JSON | 2051 |
| Más información | 2052 |
| AWSIoTRoboRunnerReadOnly | 2052 |
| Uso de la política | 2052 |
| Información de la política | 2052 |
| Versión de la política | 2052 |
| Documento de política JSON | 2053 |
| Más información | 2053 |
| AWSIoTRoboRunnerServiceRolePolicy | 2053 |
| Uso de la política | 2054 |
| Información de la política | 2054 |
| Versión de la política | 2054 |
| Documento de política JSON | 2054 |
| Más información | 2055 |
| AWSIoTRuleActions | 2055 |
| Uso de la política | 2055 |
| Información de la política | 2055 |
| Versión de la política | 2055 |
| Documento de política JSON | 2055 |
| Más información | 2056 |
| AWSIoTSiteWiseConsoleFullAccess | 2056 |
| Uso de la política | 2056 |
| Información de la política | 2057 |
| Versión de la política | 2057 |
| Documento de política JSON | 2057 |
| Más información | 2059 |
| AWSIoTSiteWiseFullAccess | 2059 |
| Uso de la política | 2059 |
| Información de la política | 2059 |
| Versión de la política | 2060 |
| Documento de política JSON | 2060 |
| Más información | 2060 |

| | |
|--|------|
| AWSIoTSiteWiseMonitorPortalAccess | 2061 |
| Uso de la política | 2061 |
| Información de la política | 2061 |
| Versión de la política | 2061 |
| Documento de política JSON | 2061 |
| Más información | 2062 |
| AWSIoTSiteWiseMonitorServiceRolePolicy | 2062 |
| Uso de la política | 2063 |
| Información de la política | 2063 |
| Versión de la política | 2063 |
| Documento de política JSON | 2063 |
| Más información | 2064 |
| AWSIoTSiteWiseReadOnlyAccess | 2064 |
| Uso de la política | 2064 |
| Información de la política | 2065 |
| Versión de la política | 2065 |
| Documento de política JSON | 2065 |
| Más información | 2065 |
| AWSIoTThingsRegistration | 2066 |
| Uso de la política | 2066 |
| Información de la política | 2066 |
| Versión de la política | 2066 |
| Documento de política JSON | 2066 |
| Más información | 2067 |
| AWSIoTThingMakerServiceRolePolicy | 2068 |
| Uso de la política | 2068 |
| Información de la política | 2068 |
| Versión de la política | 2068 |
| Documento de política JSON | 2068 |
| Más información | 2070 |
| AWSIoTWirelessDataAccess | 2070 |
| Uso de la política | 2070 |
| Información de la política | 2070 |
| Versión de la política | 2070 |
| Documento de política JSON | 2071 |
| Más información | 2071 |

| | |
|--|------|
| AWSIoTWirelessFullAccess | 2071 |
| Uso de la política | 2071 |
| Información de la política | 2072 |
| Versión de la política | 2072 |
| Documento de política JSON | 2072 |
| Más información | 2072 |
| AWSIoTWirelessFullPublishAccess | 2073 |
| Uso de la política | 2073 |
| Información de la política | 2073 |
| Versión de la política | 2073 |
| Documento de política JSON | 2073 |
| Más información | 2074 |
| AWSIoTWirelessGatewayCertManager | 2074 |
| Uso de la política | 2074 |
| Información de la política | 2074 |
| Versión de la política | 2074 |
| Documento de política JSON | 2074 |
| Más información | 2075 |
| AWSIoTWirelessLogging | 2075 |
| Uso de la política | 2075 |
| Información de la política | 2075 |
| Versión de la política | 2076 |
| Documento de política JSON | 2076 |
| Más información | 2076 |
| AWSIoTWirelessReadOnlyAccess | 2077 |
| Uso de la política | 2077 |
| Información de la política | 2077 |
| Versión de la política | 2077 |
| Documento de política JSON | 2077 |
| Más información | 2078 |
| AWSIPAMServiceRolePolicy | 2078 |
| Uso de la política | 2078 |
| Información de la política | 2078 |
| Versión de la política | 2078 |
| Documento de política JSON | 2079 |
| Más información | 2080 |

| | |
|---|------|
| AWSIQContractServiceRolePolicy | 2080 |
| Uso de la política | 2080 |
| Información de la política | 2080 |
| Versión de la política | 2080 |
| Documento de política JSON | 2081 |
| Más información | 2081 |
| AWSIQFullAccess | 2081 |
| Uso de la política | 2081 |
| Información de la política | 2081 |
| Versión de la política | 2082 |
| Documento de política JSON | 2082 |
| Más información | 2082 |
| AWSIQPermissionServiceRolePolicy | 2083 |
| Uso de la política | 2083 |
| Información de la política | 2083 |
| Versión de la política | 2083 |
| Documento de política JSON | 2083 |
| Más información | 2084 |
| AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy | 2084 |
| Uso de la política | 2085 |
| Información de la política | 2085 |
| Versión de la política | 2085 |
| Documento de política JSON | 2085 |
| Más información | 2086 |
| AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy | 2086 |
| Uso de la política | 2086 |
| Información de la política | 2086 |
| Versión de la política | 2086 |
| Documento de política JSON | 2087 |
| Más información | 2087 |
| AWSKeyManagementServicePowerUser | 2087 |
| Uso de la política | 2087 |
| Información de la política | 2087 |
| Versión de la política | 2088 |
| Documento de política JSON | 2088 |
| Más información | 2088 |

| | |
|---|------|
| AWSLakeFormationCrossAccountManager | 2089 |
| Uso de la política | 2089 |
| Información de la política | 2089 |
| Versión de la política | 2089 |
| Documento de política JSON | 2089 |
| Más información | 2091 |
| AWSLakeFormationDataAdmin | 2091 |
| Uso de la política | 2092 |
| Información de la política | 2092 |
| Versión de la política | 2092 |
| Documento de política JSON | 2092 |
| Más información | 2093 |
| AWSLambda_FullAccess | 2094 |
| Uso de la política | 2094 |
| Información de la política | 2094 |
| Versión de la política | 2094 |
| Documento de política JSON | 2094 |
| Más información | 2096 |
| AWSLambda_ReadOnlyAccess | 2096 |
| Uso de la política | 2096 |
| Información de la política | 2096 |
| Versión de la política | 2096 |
| Documento de política JSON | 2096 |
| Más información | 2098 |
| AWSLambdaBasicExecutionRole | 2098 |
| Uso de la política | 2098 |
| Información de la política | 2098 |
| Versión de la política | 2098 |
| Documento de política JSON | 2099 |
| Más información | 2099 |
| AWSLambdaDynamoDBExecutionRole | 2099 |
| Uso de la política | 2099 |
| Información de la política | 2100 |
| Versión de la política | 2100 |
| Documento de política JSON | 2100 |
| Más información | 2101 |

| | |
|-------------------------------------|------|
| AWSLambdaENIManagementAccess | 2101 |
| Uso de la política | 2101 |
| Información de la política | 2101 |
| Versión de la política | 2101 |
| Documento de política JSON | 2101 |
| Más información | 2102 |
| AWSLambdaExecute | 2102 |
| Uso de la política | 2102 |
| Información de la política | 2102 |
| Versión de la política | 2103 |
| Documento de política JSON | 2103 |
| Más información | 2103 |
| AWSLambdaFullAccess | 2104 |
| Uso de la política | 2104 |
| Información de la política | 2104 |
| Versión de la política | 2104 |
| Documento de política JSON | 2104 |
| Más información | 2106 |
| AWSLambdaInvocation-DynamoDB | 2106 |
| Uso de la política | 2106 |
| Información de la política | 2106 |
| Versión de la política | 2107 |
| Documento de política JSON | 2107 |
| Más información | 2107 |
| AWSLambdaKinesisExecutionRole | 2108 |
| Uso de la política | 2108 |
| Información de la política | 2108 |
| Versión de la política | 2108 |
| Documento de política JSON | 2108 |
| Más información | 2109 |
| AWSLambdaMSKExecutionRole | 2109 |
| Uso de la política | 2109 |
| Información de la política | 2109 |
| Versión de la política | 2110 |
| Documento de política JSON | 2110 |
| Más información | 2110 |

| | |
|--|------|
| AWSLambdaReplicator | 2111 |
| Uso de la política | 2111 |
| Información de la política | 2111 |
| Versión de la política | 2111 |
| Documento de política JSON | 2111 |
| Más información | 2112 |
| AWSLambdaRole | 2113 |
| Uso de la política | 2113 |
| Información de la política | 2113 |
| Versión de la política | 2113 |
| Documento de política JSON | 2113 |
| Más información | 2114 |
| AWSLambdaSQSQueueExecutionRole | 2114 |
| Uso de la política | 2114 |
| Información de la política | 2114 |
| Versión de la política | 2114 |
| Documento de política JSON | 2115 |
| Más información | 2115 |
| AWSLambdaVPCLambdaAccessExecutionRole | 2115 |
| Uso de la política | 2115 |
| Información de la política | 2116 |
| Versión de la política | 2116 |
| Documento de política JSON | 2116 |
| Más información | 2117 |
| AWSLicenseManagerConsumptionPolicy | 2117 |
| Uso de la política | 2117 |
| Información de la política | 2117 |
| Versión de la política | 2117 |
| Documento de política JSON | 2118 |
| Más información | 2118 |
| AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy | 2118 |
| Uso de la política | 2118 |
| Información de la política | 2119 |
| Versión de la política | 2119 |
| Documento de política JSON | 2119 |
| Más información | 2120 |

| | |
|---|------|
| AWSLicenseManagerMasterAccountRolePolicy | 2120 |
| Uso de la política | 2120 |
| Información de la política | 2120 |
| Versión de la política | 2121 |
| Documento de política JSON | 2121 |
| Más información | 2126 |
| AWSLicenseManagerMemberAccountRolePolicy | 2126 |
| Uso de la política | 2126 |
| Información de la política | 2126 |
| Versión de la política | 2126 |
| Documento de política JSON | 2126 |
| Más información | 2127 |
| AWSLicenseManagerServiceRolePolicy | 2128 |
| Uso de la política | 2128 |
| Información de la política | 2128 |
| Versión de la política | 2128 |
| Documento de política JSON | 2128 |
| Más información | 2132 |
| AWSLicenseManagerUserSubscriptionsServiceRolePolicy | 2132 |
| Uso de la política | 2132 |
| Información de la política | 2132 |
| Versión de la política | 2132 |
| Documento de política JSON | 2132 |
| Más información | 2134 |
| AWSM2ServicePolicy | 2135 |
| Uso de la política | 2135 |
| Información de la política | 2135 |
| Versión de la política | 2135 |
| Documento de política JSON | 2135 |
| Más información | 2137 |
| AWSMangedServices_ContactsServiceRolePolicy | 2137 |
| Uso de la política | 2137 |
| Información de la política | 2137 |
| Versión de la política | 2137 |
| Documento de política JSON | 2137 |
| Más información | 2138 |

| | |
|--|------|
| AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy | 2138 |
| Uso de la política | 2139 |
| Información de la política | 2139 |
| Versión de la política | 2139 |
| Documento de política JSON | 2139 |
| Más información | 2141 |
| AWSManagedServices_EventsServiceRolePolicy | 2141 |
| Uso de la política | 2141 |
| Información de la política | 2141 |
| Versión de la política | 2141 |
| Documento de política JSON | 2141 |
| Más información | 2142 |
| AWSManagedServicesDeploymentToolkitPolicy | 2142 |
| Uso de la política | 2142 |
| Información de la política | 2143 |
| Versión de la política | 2143 |
| Documento de política JSON | 2143 |
| Más información | 2145 |
| AWSMarketplaceAmiIngestion | 2145 |
| Uso de la política | 2145 |
| Información de la política | 2145 |
| Versión de la política | 2146 |
| Documento de política JSON | 2146 |
| Más información | 2146 |
| AWSMarketplaceDeploymentServiceRolePolicy | 2147 |
| Uso de la política | 2147 |
| Información de la política | 2147 |
| Versión de la política | 2147 |
| Documento de política JSON | 2147 |
| Más información | 2149 |
| AWSMarketplaceFullAccess | 2149 |
| Uso de la política | 2149 |
| Información de la política | 2149 |
| Versión de la política | 2149 |
| Documento de política JSON | 2150 |
| Más información | 2153 |

| | |
|--|------|
| AWSMarketplaceGetEntitlements | 2153 |
| Uso de la política | 2153 |
| Información de la política | 2153 |
| Versión de la política | 2153 |
| Documento de política JSON | 2154 |
| Más información | 2154 |
| AWSMarketplaceImageBuildFullAccess | 2154 |
| Uso de la política | 2154 |
| Información de la política | 2155 |
| Versión de la política | 2155 |
| Documento de política JSON | 2155 |
| Más información | 2158 |
| AWSMarketplaceLicenseManagementServiceRolePolicy | 2159 |
| Uso de la política | 2159 |
| Información de la política | 2159 |
| Versión de la política | 2159 |
| Documento de política JSON | 2159 |
| Más información | 2160 |
| AWSMarketplaceManageSubscriptions | 2160 |
| Uso de la política | 2160 |
| Información de la política | 2160 |
| Versión de la política | 2161 |
| Documento de política JSON | 2161 |
| Más información | 2162 |
| AWSMarketplaceMeteringFullAccess | 2162 |
| Uso de la política | 2162 |
| Información de la política | 2162 |
| Versión de la política | 2162 |
| Documento de política JSON | 2163 |
| Más información | 2163 |
| AWSMarketplaceMeteringRegisterUsage | 2163 |
| Uso de la política | 2163 |
| Información de la política | 2163 |
| Versión de la política | 2164 |
| Documento de política JSON | 2164 |
| Más información | 2164 |

| | |
|--|------|
| AWSMarketplaceProcurementSystemAdminFullAccess | 2165 |
| Uso de la política | 2165 |
| Información de la política | 2165 |
| Versión de la política | 2165 |
| Documento de política JSON | 2165 |
| Más información | 2166 |
| AWSMarketplacePurchaseOrdersServiceRolePolicy | 2166 |
| Uso de la política | 2166 |
| Información de la política | 2166 |
| Versión de la política | 2167 |
| Documento de política JSON | 2167 |
| Más información | 2167 |
| AWSMarketplaceRead-only | 2167 |
| Uso de la política | 2168 |
| Información de la política | 2168 |
| Versión de la política | 2168 |
| Documento de política JSON | 2168 |
| Más información | 2169 |
| AWSMarketplaceResaleAuthorizationServiceRolePolicy | 2170 |
| Uso de la política | 2170 |
| Información de la política | 2170 |
| Versión de la política | 2170 |
| Documento de política JSON | 2170 |
| Más información | 2173 |
| AWSMarketplaceSellerFullAccess | 2173 |
| Uso de la política | 2173 |
| Información de la política | 2173 |
| Versión de la política | 2173 |
| Documento de política JSON | 2173 |
| Más información | 2177 |
| AWSMarketplaceSellerProductsFullAccess | 2177 |
| Uso de la política | 2177 |
| Información de la política | 2177 |
| Versión de la política | 2178 |
| Documento de política JSON | 2178 |
| Más información | 2180 |

| | |
|--|------|
| AWSMarketplaceSellerProductsReadOnly | 2180 |
| Uso de la política | 2180 |
| Información de la política | 2180 |
| Versión de la política | 2180 |
| Documento de política JSON | 2180 |
| Más información | 2181 |
| AWSMediaConnectServicePolicy | 2181 |
| Uso de la política | 2182 |
| Información de la política | 2182 |
| Versión de la política | 2182 |
| Documento de política JSON | 2182 |
| Más información | 2183 |
| AWSMediaTailorServiceRolePolicy | 2184 |
| Uso de la política | 2184 |
| Información de la política | 2184 |
| Versión de la política | 2184 |
| Documento de política JSON | 2184 |
| Más información | 2185 |
| AWSMigrationHubDiscoveryAccess | 2185 |
| Uso de la política | 2185 |
| Información de la política | 2185 |
| Versión de la política | 2185 |
| Documento de política JSON | 2186 |
| Más información | 2187 |
| AWSMigrationHubDMSAccess | 2187 |
| Uso de la política | 2187 |
| Información de la política | 2187 |
| Versión de la política | 2188 |
| Documento de política JSON | 2188 |
| Más información | 2189 |
| AWSMigrationHubFullAccess | 2189 |
| Uso de la política | 2189 |
| Información de la política | 2189 |
| Versión de la política | 2189 |
| Documento de política JSON | 2190 |
| Más información | 2191 |

| | |
|--|------|
| AWSMigrationHubOrchestratorConsoleFullAccess | 2191 |
| Uso de la política | 2192 |
| Información de la política | 2192 |
| Versión de la política | 2192 |
| Documento de política JSON | 2192 |
| Más información | 2195 |
| AWSMigrationHubOrchestratorInstanceRolePolicy | 2195 |
| Uso de la política | 2196 |
| Información de la política | 2196 |
| Versión de la política | 2196 |
| Documento de política JSON | 2196 |
| Más información | 2197 |
| AWSMigrationHubOrchestratorPlugin | 2197 |
| Uso de la política | 2197 |
| Información de la política | 2197 |
| Versión de la política | 2197 |
| Documento de política JSON | 2198 |
| Más información | 2199 |
| AWSMigrationHubOrchestratorServiceRolePolicy | 2199 |
| Uso de la política | 2199 |
| Información de la política | 2199 |
| Versión de la política | 2200 |
| Documento de política JSON | 2200 |
| Más información | 2203 |
| AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess | 2204 |
| Uso de la política | 2204 |
| Información de la política | 2204 |
| Versión de la política | 2204 |
| Documento de política JSON | 2204 |
| Más información | 2209 |
| AWSMigrationHubRefactorSpaces-SSMAutomationPolicy | 2210 |
| Uso de la política | 2210 |
| Información de la política | 2210 |
| Versión de la política | 2210 |
| Documento de política JSON | 2210 |
| Más información | 2212 |

| | |
|--|------|
| AWSMigrationHubRefactorSpacesFullAccess | 2212 |
| Uso de la política | 2212 |
| Información de la política | 2212 |
| Versión de la política | 2213 |
| Documento de política JSON | 2213 |
| Más información | 2219 |
| AWSMigrationHubRefactorSpacesServiceRolePolicy | 2219 |
| Uso de la política | 2219 |
| Información de la política | 2219 |
| Versión de la política | 2219 |
| Documento de política JSON | 2220 |
| Más información | 2223 |
| AWSMigrationHubSMSAccess | 2223 |
| Uso de la política | 2224 |
| Información de la política | 2224 |
| Versión de la política | 2224 |
| Documento de política JSON | 2224 |
| Más información | 2225 |
| AWSMigrationHubStrategyCollector | 2225 |
| Uso de la política | 2226 |
| Información de la política | 2226 |
| Versión de la política | 2226 |
| Documento de política JSON | 2226 |
| Más información | 2228 |
| AWSMigrationHubStrategyConsoleFullAccess | 2228 |
| Uso de la política | 2229 |
| Información de la política | 2229 |
| Versión de la política | 2229 |
| Documento de política JSON | 2229 |
| Más información | 2231 |
| AWSMigrationHubStrategyServiceRolePolicy | 2231 |
| Uso de la política | 2231 |
| Información de la política | 2231 |
| Versión de la política | 2232 |
| Documento de política JSON | 2232 |
| Más información | 2233 |

| | |
|--|------|
| AWSMobileHub_FullAccess | 2233 |
| Uso de la política | 2233 |
| Información de la política | 2233 |
| Versión de la política | 2233 |
| Documento de política JSON | 2234 |
| Más información | 2235 |
| AWSMobileHub_ReadOnly | 2235 |
| Uso de la política | 2235 |
| Información de la política | 2236 |
| Versión de la política | 2236 |
| Documento de política JSON | 2236 |
| Más información | 2237 |
| AWSMSKReplicatorExecutionRole | 2237 |
| Uso de la política | 2237 |
| Información de la política | 2238 |
| Versión de la política | 2238 |
| Documento de política JSON | 2238 |
| Más información | 2239 |
| AWSNetworkFirewallServiceRolePolicy | 2240 |
| Uso de la política | 2240 |
| Información de la política | 2240 |
| Versión de la política | 2240 |
| Documento de política JSON | 2240 |
| Más información | 2242 |
| AWSNetworkManagerCloudWANServiceRolePolicy | 2242 |
| Uso de la política | 2242 |
| Información de la política | 2242 |
| Versión de la política | 2242 |
| Documento de política JSON | 2243 |
| Más información | 2243 |
| AWSNetworkManagerFullAccess | 2243 |
| Uso de la política | 2243 |
| Información de la política | 2243 |
| Versión de la política | 2244 |
| Documento de política JSON | 2244 |
| Más información | 2245 |

| | |
|--|------|
| AWSNetworkManagerReadOnlyAccess | 2245 |
| Uso de la política | 2245 |
| Información de la política | 2245 |
| Versión de la política | 2245 |
| Documento de política JSON | 2245 |
| Más información | 2246 |
| AWSNetworkManagerServiceRolePolicy | 2246 |
| Uso de la política | 2246 |
| Información de la política | 2246 |
| Versión de la política | 2247 |
| Documento de política JSON | 2247 |
| Más información | 2248 |
| AWSOpsWorks_FullAccess | 2248 |
| Uso de la política | 2248 |
| Información de la política | 2248 |
| Versión de la política | 2248 |
| Documento de política JSON | 2249 |
| Más información | 2250 |
| AWSOpsWorksCloudWatchLogs | 2250 |
| Uso de la política | 2250 |
| Información de la política | 2250 |
| Versión de la política | 2250 |
| Documento de política JSON | 2251 |
| Más información | 2251 |
| AWSOpsWorksCMInstanceProfileRole | 2251 |
| Uso de la política | 2251 |
| Información de la política | 2252 |
| Versión de la política | 2252 |
| Documento de política JSON | 2252 |
| Más información | 2253 |
| AWSOpsWorksCMServiceRole | 2253 |
| Uso de la política | 2253 |
| Información de la política | 2253 |
| Versión de la política | 2254 |
| Documento de política JSON | 2254 |
| Más información | 2258 |

| | |
|--|------|
| AWSOpsWorksInstanceRegistration | 2258 |
| Uso de la política | 2258 |
| Información de la política | 2258 |
| Versión de la política | 2259 |
| Documento de política JSON | 2259 |
| Más información | 2259 |
| AWSOpsWorksRegisterCLI_EC2 | 2260 |
| Uso de la política | 2260 |
| Información de la política | 2260 |
| Versión de la política | 2260 |
| Documento de política JSON | 2260 |
| Más información | 2261 |
| AWSOpsWorksRegisterCLI_OnPremises | 2261 |
| Uso de la política | 2261 |
| Información de la política | 2261 |
| Versión de la política | 2262 |
| Documento de política JSON | 2262 |
| Más información | 2263 |
| AWSOrganizationsFullAccess | 2264 |
| Uso de la política | 2264 |
| Información de la política | 2264 |
| Versión de la política | 2264 |
| Documento de política JSON | 2264 |
| Más información | 2265 |
| AWSOrganizationsReadOnlyAccess | 2266 |
| Uso de la política | 2266 |
| Información de la política | 2266 |
| Versión de la política | 2266 |
| Documento de política JSON | 2266 |
| Más información | 2267 |
| AWSOrganizationsServiceTrustPolicy | 2267 |
| Uso de la política | 2267 |
| Información de la política | 2267 |
| Versión de la política | 2268 |
| Documento de política JSON | 2268 |
| Más información | 2268 |

| | |
|---|------|
| AWSOutpostsAuthorizeServerPolicy | 2269 |
| Uso de la política | 2269 |
| Información de la política | 2269 |
| Versión de la política | 2269 |
| Documento de política JSON | 2269 |
| Más información | 2270 |
| AWSOutpostsServiceRolePolicy | 2270 |
| Uso de la política | 2270 |
| Información de la política | 2270 |
| Versión de la política | 2270 |
| Documento de política JSON | 2271 |
| Más información | 2271 |
| AWSPanoramaApplianceRolePolicy | 2271 |
| Uso de la política | 2271 |
| Información de la política | 2271 |
| Versión de la política | 2272 |
| Documento de política JSON | 2272 |
| Más información | 2272 |
| AWSPanoramaApplianceServiceRolePolicy | 2273 |
| Uso de la política | 2273 |
| Información de la política | 2273 |
| Versión de la política | 2273 |
| Documento de política JSON | 2273 |
| Más información | 2275 |
| AWSPanoramaFullAccess | 2275 |
| Uso de la política | 2275 |
| Información de la política | 2275 |
| Versión de la política | 2276 |
| Documento de política JSON | 2276 |
| Más información | 2278 |
| AWSPanoramaGreengrassGroupRolePolicy | 2278 |
| Uso de la política | 2279 |
| Información de la política | 2279 |
| Versión de la política | 2279 |
| Documento de política JSON | 2279 |
| Más información | 2280 |

| | |
|--|------|
| AWSPanoramaSageMakerRolePolicy | 2281 |
| Uso de la política | 2281 |
| Información de la política | 2281 |
| Versión de la política | 2281 |
| Documento de política JSON | 2281 |
| Más información | 2282 |
| AWSPanoramaServiceLinkedRolePolicy | 2282 |
| Uso de la política | 2282 |
| Información de la política | 2282 |
| Versión de la política | 2283 |
| Documento de política JSON | 2283 |
| Más información | 2285 |
| AWSPanoramaServiceRolePolicy | 2286 |
| Uso de la política | 2286 |
| Información de la política | 2286 |
| Versión de la política | 2286 |
| Documento de política JSON | 2286 |
| Más información | 2293 |
| AWSPriceListServiceFullAccess | 2293 |
| Uso de la política | 2294 |
| Información de la política | 2294 |
| Versión de la política | 2294 |
| Documento de política JSON | 2294 |
| Más información | 2294 |
| AWSPrivateCAAuditor | 2295 |
| Uso de la política | 2295 |
| Información de la política | 2295 |
| Versión de la política | 2295 |
| Documento de política JSON | 2295 |
| Más información | 2296 |
| AWSPrivateCAFullAccess | 2296 |
| Uso de la política | 2296 |
| Información de la política | 2297 |
| Versión de la política | 2297 |
| Documento de política JSON | 2297 |
| Más información | 2297 |

| | |
|---|------|
| AWSPriateCAPrivilegedUser | 2298 |
| Uso de la política | 2298 |
| Información de la política | 2298 |
| Versión de la política | 2298 |
| Documento de política JSON | 2298 |
| Más información | 2299 |
| AWSPriateCARedOnly | 2300 |
| Uso de la política | 2300 |
| Información de la política | 2300 |
| Versión de la política | 2300 |
| Documento de política JSON | 2300 |
| Más información | 2301 |
| AWSPriateCAUser | 2301 |
| Uso de la política | 2301 |
| Información de la política | 2301 |
| Versión de la política | 2301 |
| Documento de política JSON | 2302 |
| Más información | 2303 |
| AWSPriateMarketplaceAdminFullAccess | 2303 |
| Uso de la política | 2303 |
| Información de la política | 2303 |
| Versión de la política | 2304 |
| Documento de política JSON | 2304 |
| Más información | 2305 |
| AWSPriateMarketplaceRequests | 2305 |
| Uso de la política | 2306 |
| Información de la política | 2306 |
| Versión de la política | 2306 |
| Documento de política JSON | 2306 |
| Más información | 2307 |
| AWSPriateNetworksServiceRolePolicy | 2307 |
| Uso de la política | 2307 |
| Información de la política | 2307 |
| Versión de la política | 2307 |
| Documento de política JSON | 2308 |
| Más información | 2308 |

| | |
|---|------|
| AWSProtonCodeBuildProvisioningBasicAccess | 2308 |
| Uso de la política | 2308 |
| Información de la política | 2308 |
| Versión de la política | 2309 |
| Documento de política JSON | 2309 |
| Más información | 2309 |
| AWSProtonCodeBuildProvisioningServiceRolePolicy | 2310 |
| Uso de la política | 2310 |
| Información de la política | 2310 |
| Versión de la política | 2310 |
| Documento de política JSON | 2310 |
| Más información | 2312 |
| AWSProtonDeveloperAccess | 2312 |
| Uso de la política | 2312 |
| Información de la política | 2312 |
| Versión de la política | 2312 |
| Documento de política JSON | 2313 |
| Más información | 2314 |
| AWSProtonFullAccess | 2315 |
| Uso de la política | 2315 |
| Información de la política | 2315 |
| Versión de la política | 2315 |
| Documento de política JSON | 2315 |
| Más información | 2317 |
| AWSProtonReadOnlyAccess | 2317 |
| Uso de la política | 2317 |
| Información de la política | 2317 |
| Versión de la política | 2318 |
| Documento de política JSON | 2318 |
| Más información | 2319 |
| AWSProtonServiceGitSyncServiceRolePolicy | 2320 |
| Uso de la política | 2320 |
| Información de la política | 2320 |
| Versión de la política | 2320 |
| Documento de política JSON | 2320 |
| Más información | 2321 |

| | |
|--|------|
| AWSProtonSyncServiceRolePolicy | 2321 |
| Uso de la política | 2321 |
| Información de la política | 2321 |
| Versión de la política | 2322 |
| Documento de política JSON | 2322 |
| Más información | 2323 |
| AWSPurchaseOrdersServiceRolePolicy | 2323 |
| Uso de la política | 2323 |
| Información de la política | 2323 |
| Versión de la política | 2323 |
| Documento de política JSON | 2324 |
| Más información | 2324 |
| AWSQuicksightAthenaAccess | 2325 |
| Uso de la política | 2325 |
| Información de la política | 2325 |
| Versión de la política | 2325 |
| Documento de política JSON | 2325 |
| Más información | 2328 |
| AWSQuickSightDescribeRDS | 2328 |
| Uso de la política | 2328 |
| Información de la política | 2328 |
| Versión de la política | 2328 |
| Documento de política JSON | 2328 |
| Más información | 2329 |
| AWSQuickSightDescribeRedshift | 2329 |
| Uso de la política | 2329 |
| Información de la política | 2329 |
| Versión de la política | 2330 |
| Documento de política JSON | 2330 |
| Más información | 2330 |
| AWSQuickSightElasticsearchPolicy | 2330 |
| Uso de la política | 2331 |
| Información de la política | 2331 |
| Versión de la política | 2331 |
| Documento de política JSON | 2331 |
| Más información | 2332 |

| | |
|--|------|
| AWSQuickSightIoTAnalyticsAccess | 2332 |
| Uso de la política | 2333 |
| Información de la política | 2333 |
| Versión de la política | 2333 |
| Documento de política JSON | 2333 |
| Más información | 2334 |
| AWSQuickSightListIAM | 2334 |
| Uso de la política | 2334 |
| Información de la política | 2334 |
| Versión de la política | 2334 |
| Documento de política JSON | 2334 |
| Más información | 2335 |
| AWSQuickSightOpenSearchPolicy | 2335 |
| Uso de la política | 2335 |
| Información de la política | 2335 |
| Versión de la política | 2336 |
| Documento de política JSON | 2336 |
| Más información | 2337 |
| AWSQuickSightSageMakerPolicy | 2337 |
| Uso de la política | 2337 |
| Información de la política | 2337 |
| Versión de la política | 2337 |
| Documento de política JSON | 2338 |
| Más información | 2339 |
| AWSQuickSightTimestreamPolicy | 2339 |
| Uso de la política | 2339 |
| Información de la política | 2339 |
| Versión de la política | 2340 |
| Documento de política JSON | 2340 |
| Más información | 2340 |
| AWSReachabilityAnalyzerServiceRolePolicy | 2341 |
| Uso de la política | 2341 |
| Información de la política | 2341 |
| Versión de la política | 2341 |
| Documento de política JSON | 2341 |
| Más información | 2344 |

| | |
|---|------|
| AWSRefactoringToolkitFullAccess | 2344 |
| Uso de la política | 2344 |
| Información de la política | 2344 |
| Versión de la política | 2344 |
| Documento de política JSON | 2345 |
| Más información | 2358 |
| AWSRefactoringToolkitSidecarPolicy | 2358 |
| Uso de la política | 2358 |
| Información de la política | 2359 |
| Versión de la política | 2359 |
| Documento de política JSON | 2359 |
| Más información | 2360 |
| AWSRePostPrivateCloudWatchAccess | 2360 |
| Uso de la política | 2360 |
| Información de la política | 2360 |
| Versión de la política | 2361 |
| Documento de política JSON | 2361 |
| Más información | 2361 |
| AWSRepostSpaceSupportOperationsPolicy | 2362 |
| Uso de la política | 2362 |
| Información de la política | 2362 |
| Versión de la política | 2362 |
| Documento de política JSON | 2362 |
| Más información | 2363 |
| AWSResilienceHubAssessmentExecutionPolicy | 2363 |
| Uso de la política | 2363 |
| Información de la política | 2363 |
| Versión de la política | 2363 |
| Documento de política JSON | 2364 |
| Más información | 2368 |
| AWSResourceAccessManagerFullAccess | 2368 |
| Uso de la política | 2368 |
| Información de la política | 2368 |
| Versión de la política | 2368 |
| Documento de política JSON | 2368 |
| Más información | 2369 |

| | |
|--|------|
| AWSResourceAccessManagerReadOnlyAccess | 2369 |
| Uso de la política | 2369 |
| Información de la política | 2369 |
| Versión de la política | 2370 |
| Documento de política JSON | 2370 |
| Más información | 2370 |
| AWSResourceAccessManagerResourceShareParticipantAccess | 2370 |
| Uso de la política | 2371 |
| Información de la política | 2371 |
| Versión de la política | 2371 |
| Documento de política JSON | 2371 |
| Más información | 2372 |
| AWSResourceAccessManagerServiceRolePolicy | 2372 |
| Uso de la política | 2372 |
| Información de la política | 2372 |
| Versión de la política | 2372 |
| Documento de política JSON | 2373 |
| Más información | 2373 |
| AWSResourceExplorerFullAccess | 2374 |
| Uso de la política | 2374 |
| Información de la política | 2374 |
| Versión de la política | 2374 |
| Documento de política JSON | 2374 |
| Más información | 2375 |
| AWSResourceExplorerOrganizationsAccess | 2375 |
| Uso de la política | 2376 |
| Información de la política | 2376 |
| Versión de la política | 2376 |
| Documento de política JSON | 2376 |
| Más información | 2378 |
| AWSResourceExplorerReadOnlyAccess | 2378 |
| Uso de la política | 2378 |
| Información de la política | 2378 |
| Versión de la política | 2378 |
| Documento de política JSON | 2379 |
| Más información | 2379 |

| | |
|--|------|
| AWSResourceExplorerServiceRolePolicy | 2379 |
| Uso de la política | 2380 |
| Información de la política | 2380 |
| Versión de la política | 2380 |
| Documento de política JSON | 2380 |
| Más información | 2389 |
| AWSResourceGroupsReadOnlyAccess | 2389 |
| Uso de la política | 2389 |
| Información de la política | 2390 |
| Versión de la política | 2390 |
| Documento de política JSON | 2390 |
| Más información | 2391 |
| AWSRoboMaker_FullAccess | 2392 |
| Uso de la política | 2392 |
| Información de la política | 2392 |
| Versión de la política | 2392 |
| Documento de política JSON | 2392 |
| Más información | 2393 |
| AWSRoboMakerReadOnlyAccess | 2394 |
| Uso de la política | 2394 |
| Información de la política | 2394 |
| Versión de la política | 2394 |
| Documento de política JSON | 2394 |
| Más información | 2395 |
| AWSRoboMakerServicePolicy | 2395 |
| Uso de la política | 2395 |
| Información de la política | 2395 |
| Versión de la política | 2396 |
| Documento de política JSON | 2396 |
| Más información | 2397 |
| AWSRoboMakerServiceRolePolicy | 2398 |
| Uso de la política | 2398 |
| Información de la política | 2398 |
| Versión de la política | 2398 |
| Documento de política JSON | 2398 |
| Más información | 2399 |

| | |
|---|------|
| AWSRolesAnywhereServicePolicy | 2400 |
| Uso de la política | 2400 |
| Información de la política | 2400 |
| Versión de la política | 2400 |
| Documento de política JSON | 2400 |
| Más información | 2401 |
| AWSS3OnOutpostsServiceRolePolicy | 2401 |
| Uso de la política | 2401 |
| Información de la política | 2402 |
| Versión de la política | 2402 |
| Documento de política JSON | 2402 |
| Más información | 2405 |
| AWSSavingsPlansFullAccess | 2405 |
| Uso de la política | 2405 |
| Información de la política | 2405 |
| Versión de la política | 2405 |
| Documento de política JSON | 2405 |
| Más información | 2406 |
| AWSSavingsPlansReadOnlyAccess | 2406 |
| Uso de la política | 2406 |
| Información de la política | 2406 |
| Versión de la política | 2406 |
| Documento de política JSON | 2407 |
| Más información | 2407 |
| AWSSecurityHubFullAccess | 2407 |
| Uso de la política | 2407 |
| Información de la política | 2407 |
| Versión de la política | 2408 |
| Documento de política JSON | 2408 |
| Más información | 2409 |
| AWSSecurityHubOrganizationsAccess | 2409 |
| Uso de la política | 2409 |
| Información de la política | 2409 |
| Versión de la política | 2409 |
| Documento de política JSON | 2410 |
| Más información | 2411 |

| | |
|--|------|
| AWSSecurityHubReadOnlyAccess | 2411 |
| Uso de la política | 2411 |
| Información de la política | 2411 |
| Versión de la política | 2412 |
| Documento de política JSON | 2412 |
| Más información | 2412 |
| AWSSecurityHubServiceRolePolicy | 2413 |
| Uso de la política | 2413 |
| Información de la política | 2413 |
| Versión de la política | 2413 |
| Documento de política JSON | 2413 |
| Más información | 2415 |
| AWSServiceCatalogAdminFullAccess | 2415 |
| Uso de la política | 2416 |
| Información de la política | 2416 |
| Versión de la política | 2416 |
| Documento de política JSON | 2416 |
| Más información | 2419 |
| AWSServiceCatalogAdminReadOnlyAccess | 2419 |
| Uso de la política | 2419 |
| Información de la política | 2419 |
| Versión de la política | 2419 |
| Documento de política JSON | 2420 |
| Más información | 2421 |
| AWSServiceCatalogAppRegistryFullAccess | 2421 |
| Uso de la política | 2421 |
| Información de la política | 2421 |
| Versión de la política | 2422 |
| Documento de política JSON | 2422 |
| Más información | 2424 |
| AWSServiceCatalogAppRegistryReadOnlyAccess | 2424 |
| Uso de la política | 2424 |
| Información de la política | 2425 |
| Versión de la política | 2425 |
| Documento de política JSON | 2425 |
| Más información | 2426 |

| | |
|--|------|
| AWSServiceCatalogAppRegistryServiceRolePolicy | 2426 |
| Uso de la política | 2426 |
| Información de la política | 2426 |
| Versión de la política | 2426 |
| Documento de política JSON | 2427 |
| Más información | 2428 |
| AWSServiceCatalogEndUserFullAccess | 2428 |
| Uso de la política | 2428 |
| Información de la política | 2428 |
| Versión de la política | 2428 |
| Documento de política JSON | 2429 |
| Más información | 2431 |
| AWSServiceCatalogEndUserReadOnlyAccess | 2431 |
| Uso de la política | 2431 |
| Información de la política | 2431 |
| Versión de la política | 2431 |
| Documento de política JSON | 2432 |
| Más información | 2433 |
| AWSServiceCatalogOrgsDataSyncServiceRolePolicy | 2434 |
| Uso de la política | 2434 |
| Información de la política | 2434 |
| Versión de la política | 2434 |
| Documento de política JSON | 2434 |
| Más información | 2435 |
| AWSServiceCatalogSyncServiceRolePolicy | 2435 |
| Uso de la política | 2435 |
| Información de la política | 2435 |
| Versión de la política | 2435 |
| Documento de política JSON | 2436 |
| Más información | 2437 |
| AWSServiceRoleForAmazonEKSNodegroup | 2437 |
| Uso de la política | 2437 |
| Información de la política | 2437 |
| Versión de la política | 2437 |
| Documento de política JSON | 2437 |
| Más información | 2441 |

| | |
|--|------|
| AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICEPOLICY | 2442 |
| Uso de la política | 2442 |
| Información de la política | 2442 |
| Versión de la política | 2442 |
| Documento de política JSON | 2442 |
| Más información | 2443 |
| AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsSERVICEPOLICY | 2443 |
| Uso de la política | 2443 |
| Información de la política | 2443 |
| Versión de la política | 2443 |
| Documento de política JSON | 2444 |
| Más información | 2444 |
| AWSServiceRoleForCodeGuru-Profiler | 2444 |
| Uso de la política | 2444 |
| Información de la política | 2445 |
| Versión de la política | 2445 |
| Documento de política JSON | 2445 |
| Más información | 2445 |
| AWSServiceRoleForCodeWhispererPolicy | 2446 |
| Uso de la política | 2446 |
| Información de la política | 2446 |
| Versión de la política | 2446 |
| Documento de política JSON | 2446 |
| Más información | 2448 |
| AWSServiceRoleForEC2ScheduledInstances | 2448 |
| Uso de la política | 2448 |
| Información de la política | 2448 |
| Versión de la política | 2449 |
| Documento de política JSON | 2449 |
| Más información | 2450 |
| AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy | 2450 |
| Uso de la política | 2450 |
| Información de la política | 2450 |
| Versión de la política | 2450 |
| Documento de política JSON | 2451 |
| Más información | 2451 |

| | |
|--|------|
| AWSServiceRoleForImageBuilder | 2451 |
| Uso de la política | 2451 |
| Información de la política | 2451 |
| Versión de la política | 2452 |
| Documento de política JSON | 2452 |
| Más información | 2461 |
| AWSServiceRoleForIoTSiteWise | 2462 |
| Uso de la política | 2462 |
| Información de la política | 2462 |
| Versión de la política | 2462 |
| Documento de política JSON | 2462 |
| Más información | 2464 |
| AWSServiceRoleForLogDeliveryPolicy | 2464 |
| Uso de la política | 2464 |
| Información de la política | 2464 |
| Versión de la política | 2464 |
| Documento de política JSON | 2464 |
| Más información | 2465 |
| AWSServiceRoleForMonitronPolicy | 2465 |
| Uso de la política | 2465 |
| Información de la política | 2465 |
| Versión de la política | 2466 |
| Documento de política JSON | 2466 |
| Más información | 2466 |
| AWSServiceRoleForNeptuneGraphPolicy | 2467 |
| Uso de la política | 2467 |
| Información de la política | 2467 |
| Versión de la política | 2467 |
| Documento de política JSON | 2467 |
| Más información | 2469 |
| AWSServiceRoleForPrivateMarketplaceAdminPolicy | 2469 |
| Uso de la política | 2469 |
| Información de la política | 2469 |
| Versión de la política | 2469 |
| Documento de política JSON | 2469 |
| Más información | 2471 |

| | |
|---|------|
| AWSServiceRoleForSMS | 2471 |
| Uso de la política | 2471 |
| Información de la política | 2472 |
| Versión de la política | 2472 |
| Documento de política JSON | 2472 |
| Más información | 2479 |
| AWSServiceRolePolicyForBackupReports | 2479 |
| Uso de la política | 2479 |
| Información de la política | 2479 |
| Versión de la política | 2479 |
| Documento de política JSON | 2479 |
| Más información | 2481 |
| AWSServiceRolePolicyForBackupRestoreTesting | 2481 |
| Uso de la política | 2481 |
| Información de la política | 2481 |
| Versión de la política | 2481 |
| Documento de política JSON | 2482 |
| Más información | 2484 |
| AWSShieldDRTAcessPolicy | 2485 |
| Uso de la política | 2485 |
| Información de la política | 2485 |
| Versión de la política | 2485 |
| Documento de política JSON | 2485 |
| Más información | 2486 |
| AWSShieldServiceRolePolicy | 2486 |
| Uso de la política | 2487 |
| Información de la política | 2487 |
| Versión de la política | 2487 |
| Documento de política JSON | 2487 |
| Más información | 2488 |
| AWSSSMForSAPServiceLinkedRolePolicy | 2488 |
| Uso de la política | 2488 |
| Información de la política | 2488 |
| Versión de la política | 2488 |
| Documento de política JSON | 2489 |
| Más información | 2495 |

| | |
|--|------|
| AWSSSMOpsInsightsServiceRolePolicy | 2495 |
| Uso de la política | 2495 |
| Información de la política | 2495 |
| Versión de la política | 2495 |
| Documento de política JSON | 2496 |
| Más información | 2496 |
| AWSSSODirectoryAdministrator | 2497 |
| Uso de la política | 2497 |
| Información de la política | 2497 |
| Versión de la política | 2497 |
| Documento de política JSON | 2497 |
| Más información | 2498 |
| AWSSSODirectoryReadOnly | 2498 |
| Uso de la política | 2498 |
| Información de la política | 2498 |
| Versión de la política | 2498 |
| Documento de política JSON | 2499 |
| Más información | 2499 |
| AWSSSOMasterAccountAdministrator | 2499 |
| Uso de la política | 2500 |
| Información de la política | 2500 |
| Versión de la política | 2500 |
| Documento de política JSON | 2500 |
| Más información | 2502 |
| AWSSSOMemberAccountAdministrator | 2502 |
| Uso de la política | 2502 |
| Información de la política | 2502 |
| Versión de la política | 2503 |
| Documento de política JSON | 2503 |
| Más información | 2504 |
| AWSSSOReadOnly | 2504 |
| Uso de la política | 2504 |
| Información de la política | 2504 |
| Versión de la política | 2505 |
| Documento de política JSON | 2505 |
| Más información | 2506 |

| | |
|--|------|
| AWSSSOServiceRolePolicy | 2506 |
| Uso de la política | 2506 |
| Información de la política | 2506 |
| Versión de la política | 2506 |
| Documento de política JSON | 2507 |
| Más información | 2510 |
| AWSSStepFunctionsConsoleFullAccess | 2510 |
| Uso de la política | 2510 |
| Información de la política | 2510 |
| Versión de la política | 2511 |
| Documento de política JSON | 2511 |
| Más información | 2512 |
| AWSSStepFunctionsFullAccess | 2512 |
| Uso de la política | 2512 |
| Información de la política | 2512 |
| Versión de la política | 2512 |
| Documento de política JSON | 2513 |
| Más información | 2513 |
| AWSSStepFunctionsReadOnlyAccess | 2513 |
| Uso de la política | 2513 |
| Información de la política | 2513 |
| Versión de la política | 2514 |
| Documento de política JSON | 2514 |
| Más información | 2514 |
| AWSSStorageGatewayFullAccess | 2515 |
| Uso de la política | 2515 |
| Información de la política | 2515 |
| Versión de la política | 2515 |
| Documento de política JSON | 2515 |
| Más información | 2516 |
| AWSSStorageGatewayReadOnlyAccess | 2516 |
| Uso de la política | 2516 |
| Información de la política | 2516 |
| Versión de la política | 2517 |
| Documento de política JSON | 2517 |
| Más información | 2517 |

| | |
|---|------|
| AWSSStorageGatewayServiceRolePolicy | 2518 |
| Uso de la política | 2518 |
| Información de la política | 2518 |
| Versión de la política | 2518 |
| Documento de política JSON | 2518 |
| Más información | 2519 |
| AWSSupplyChainFederationAdminAccess | 2519 |
| Uso de la política | 2519 |
| Información de la política | 2519 |
| Versión de la política | 2520 |
| Documento de política JSON | 2520 |
| Más información | 2525 |
| AWSSupportAccess | 2525 |
| Uso de la política | 2525 |
| Información de la política | 2525 |
| Versión de la política | 2526 |
| Documento de política JSON | 2526 |
| Más información | 2526 |
| AWSSupportAppFullAccess | 2527 |
| Uso de la política | 2527 |
| Información de la política | 2527 |
| Versión de la política | 2527 |
| Documento de política JSON | 2527 |
| Más información | 2528 |
| AWSSupportAppReadOnlyAccess | 2528 |
| Uso de la política | 2528 |
| Información de la política | 2529 |
| Versión de la política | 2529 |
| Documento de política JSON | 2529 |
| Más información | 2529 |
| AWSSupportPlansFullAccess | 2530 |
| Uso de la política | 2530 |
| Información de la política | 2530 |
| Versión de la política | 2530 |
| Documento de política JSON | 2530 |
| Más información | 2531 |

| | |
|--|------|
| AWSSupportPlansReadOnlyAccess | 2531 |
| Uso de la política | 2531 |
| Información de la política | 2531 |
| Versión de la política | 2531 |
| Documento de política JSON | 2532 |
| Más información | 2532 |
| AWSSupportServiceRolePolicy | 2532 |
| Uso de la política | 2533 |
| Información de la política | 2533 |
| Versión de la política | 2533 |
| Documento de política JSON | 2533 |
| Más información | 2607 |
| AWSSystemsManagerAccountDiscoveryServicePolicy | 2607 |
| Uso de la política | 2607 |
| Información de la política | 2607 |
| Versión de la política | 2607 |
| Documento de política JSON | 2608 |
| Más información | 2608 |
| AWSSystemsManagerChangeManagementServicePolicy | 2608 |
| Uso de la política | 2609 |
| Información de la política | 2609 |
| Versión de la política | 2609 |
| Documento de política JSON | 2609 |
| Más información | 2611 |
| AWSSystemsManagerForSAPFullAccess | 2611 |
| Uso de la política | 2611 |
| Información de la política | 2611 |
| Versión de la política | 2611 |
| Documento de política JSON | 2612 |
| Más información | 2612 |
| AWSSystemsManagerForSAPReadOnlyAccess | 2613 |
| Uso de la política | 2613 |
| Información de la política | 2613 |
| Versión de la política | 2613 |
| Documento de política JSON | 2613 |
| Más información | 2614 |

| | |
|--|------|
| AWSSystemsManagerOpsDataSyncServiceRolePolicy | 2614 |
| Uso de la política | 2614 |
| Información de la política | 2614 |
| Versión de la política | 2614 |
| Documento de política JSON | 2615 |
| Más información | 2618 |
| AWSThinkboxAssetServerPolicy | 2618 |
| Uso de la política | 2618 |
| Información de la política | 2619 |
| Versión de la política | 2619 |
| Documento de política JSON | 2619 |
| Más información | 2620 |
| AWSThinkboxAWSPortalAdminPolicy | 2620 |
| Uso de la política | 2620 |
| Información de la política | 2620 |
| Versión de la política | 2620 |
| Documento de política JSON | 2621 |
| Más información | 2630 |
| AWSThinkboxAWSPortalGatewayPolicy | 2631 |
| Uso de la política | 2631 |
| Información de la política | 2631 |
| Versión de la política | 2631 |
| Documento de política JSON | 2631 |
| Más información | 2633 |
| AWSThinkboxAWSPortalWorkerPolicy | 2633 |
| Uso de la política | 2633 |
| Información de la política | 2634 |
| Versión de la política | 2634 |
| Documento de política JSON | 2634 |
| Más información | 2636 |
| AWSThinkboxDeadlineResourceTrackerAccessPolicy | 2636 |
| Uso de la política | 2636 |
| Información de la política | 2636 |
| Versión de la política | 2637 |
| Documento de política JSON | 2637 |
| Más información | 2640 |

| | |
|--|------|
| AWSThinkboxDeadlineResourceTrackerAdminPolicy | 2640 |
| Uso de la política | 2640 |
| Información de la política | 2640 |
| Versión de la política | 2640 |
| Documento de política JSON | 2641 |
| Más información | 2646 |
| AWSThinkboxDeadlineSpotEventPluginAdminPolicy | 2646 |
| Uso de la política | 2646 |
| Información de la política | 2647 |
| Versión de la política | 2647 |
| Documento de política JSON | 2647 |
| Más información | 2650 |
| AWSThinkboxDeadlineSpotEventPluginWorkerPolicy | 2650 |
| Uso de la política | 2650 |
| Información de la política | 2650 |
| Versión de la política | 2650 |
| Documento de política JSON | 2651 |
| Más información | 2652 |
| AWSTransferConsoleFullAccess | 2652 |
| Uso de la política | 2652 |
| Información de la política | 2652 |
| Versión de la política | 2653 |
| Documento de política JSON | 2653 |
| Más información | 2654 |
| AWSTransferFullAccess | 2654 |
| Uso de la política | 2654 |
| Información de la política | 2654 |
| Versión de la política | 2654 |
| Documento de política JSON | 2655 |
| Más información | 2655 |
| AWSTransferLoggingAccess | 2656 |
| Uso de la política | 2656 |
| Información de la política | 2656 |
| Versión de la política | 2656 |
| Documento de política JSON | 2656 |
| Más información | 2657 |

| | |
|---|------|
| AWSTransferReadOnlyAccess | 2657 |
| Uso de la política | 2657 |
| Información de la política | 2657 |
| Versión de la política | 2657 |
| Documento de política JSON | 2658 |
| Más información | 2658 |
| AWSTrustedAdvisorPriorityFullAccess | 2658 |
| Uso de la política | 2659 |
| Información de la política | 2659 |
| Versión de la política | 2659 |
| Documento de política JSON | 2659 |
| Más información | 2661 |
| AWSTrustedAdvisorPriorityReadOnlyAccess | 2661 |
| Uso de la política | 2661 |
| Información de la política | 2661 |
| Versión de la política | 2662 |
| Documento de política JSON | 2662 |
| Más información | 2663 |
| AWSTrustedAdvisorReportingServiceRolePolicy | 2663 |
| Uso de la política | 2663 |
| Información de la política | 2663 |
| Versión de la política | 2663 |
| Documento de política JSON | 2664 |
| Más información | 2664 |
| AWSTrustedAdvisorServiceRolePolicy | 2664 |
| Uso de la política | 2665 |
| Información de la política | 2665 |
| Versión de la política | 2665 |
| Documento de política JSON | 2665 |
| Más información | 2668 |
| AWSUserNotificationsServiceLinkedRolePolicy | 2668 |
| Uso de la política | 2668 |
| Información de la política | 2668 |
| Versión de la política | 2668 |
| Documento de política JSON | 2669 |
| Más información | 2669 |

| | |
|---|------|
| AWSVendorInsightsAssessorFullAccess | 2670 |
| Uso de la política | 2670 |
| Información de la política | 2670 |
| Versión de la política | 2670 |
| Documento de política JSON | 2670 |
| Más información | 2671 |
| AWSVendorInsightsAssessorReadOnly | 2672 |
| Uso de la política | 2672 |
| Información de la política | 2672 |
| Versión de la política | 2672 |
| Documento de política JSON | 2672 |
| Más información | 2673 |
| AWSVendorInsightsVendorFullAccess | 2673 |
| Uso de la política | 2673 |
| Información de la política | 2673 |
| Versión de la política | 2674 |
| Documento de política JSON | 2674 |
| Más información | 2675 |
| AWSVendorInsightsVendorReadOnly | 2676 |
| Uso de la política | 2676 |
| Información de la política | 2676 |
| Versión de la política | 2676 |
| Documento de política JSON | 2676 |
| Más información | 2677 |
| AWSVpcLatticeServiceRolePolicy | 2678 |
| Uso de la política | 2678 |
| Información de la política | 2678 |
| Versión de la política | 2678 |
| Documento de política JSON | 2678 |
| Más información | 2679 |
| AWSVPCS2SVpnServiceRolePolicy | 2679 |
| Uso de la política | 2679 |
| Información de la política | 2679 |
| Versión de la política | 2679 |
| Documento de política JSON | 2680 |
| Más información | 2680 |

| | |
|---|------|
| AWSVPCTransitGatewayServiceRolePolicy | 2680 |
| Uso de la política | 2680 |
| Información de la política | 2680 |
| Versión de la política | 2681 |
| Documento de política JSON | 2681 |
| Más información | 2681 |
| AWSVPCVerifiedAccessServiceRolePolicy | 2682 |
| Uso de la política | 2682 |
| Información de la política | 2682 |
| Versión de la política | 2682 |
| Documento de política JSON | 2682 |
| Más información | 2684 |
| AWSWAFConsoleFullAccess | 2684 |
| Uso de la política | 2684 |
| Información de la política | 2684 |
| Versión de la política | 2685 |
| Documento de política JSON | 2685 |
| Más información | 2687 |
| AWSWAFConsoleReadOnlyAccess | 2687 |
| Uso de la política | 2687 |
| Información de la política | 2687 |
| Versión de la política | 2688 |
| Documento de política JSON | 2688 |
| Más información | 2689 |
| AWSWAFFullAccess | 2689 |
| Uso de la política | 2689 |
| Información de la política | 2689 |
| Versión de la política | 2689 |
| Documento de política JSON | 2690 |
| Más información | 2691 |
| AWSWAFReadOnlyAccess | 2692 |
| Uso de la política | 2692 |
| Información de la política | 2692 |
| Versión de la política | 2692 |
| Documento de política JSON | 2692 |
| Más información | 2693 |

| | |
|--|------|
| AWSWellArchitectedDiscoveryServiceRolePolicy | 2693 |
| Uso de la política | 2693 |
| Información de la política | 2693 |
| Versión de la política | 2694 |
| Documento de política JSON | 2694 |
| Más información | 2695 |
| AWSWellArchitectedOrganizationsServiceRolePolicy | 2695 |
| Uso de la política | 2696 |
| Información de la política | 2696 |
| Versión de la política | 2696 |
| Documento de política JSON | 2696 |
| Más información | 2697 |
| AWSWickrFullAccess | 2697 |
| Uso de la política | 2697 |
| Información de la política | 2697 |
| Versión de la política | 2697 |
| Documento de política JSON | 2697 |
| Más información | 2698 |
| AWSXrayCrossAccountSharingConfiguration | 2698 |
| Uso de la política | 2698 |
| Información de la política | 2698 |
| Versión de la política | 2699 |
| Documento de política JSON | 2699 |
| Más información | 2700 |
| AWSXRayDaemonWriteAccess | 2700 |
| Uso de la política | 2700 |
| Información de la política | 2700 |
| Versión de la política | 2700 |
| Documento de política JSON | 2701 |
| Más información | 2701 |
| AWSXrayFullAccess | 2701 |
| Uso de la política | 2701 |
| Información de la política | 2702 |
| Versión de la política | 2702 |
| Documento de política JSON | 2702 |
| Más información | 2702 |

| | |
|---|------|
| AWSXrayReadOnlyAccess | 2703 |
| Uso de la política | 2703 |
| Información de la política | 2703 |
| Versión de la política | 2703 |
| Documento de política JSON | 2703 |
| Más información | 2704 |
| AWSXrayWriteOnlyAccess | 2704 |
| Uso de la política | 2704 |
| Información de la política | 2705 |
| Versión de la política | 2705 |
| Documento de política JSON | 2705 |
| Más información | 2706 |
| AWSZonalAutoshiftPracticeRunSLRPolicy | 2706 |
| Uso de la política | 2706 |
| Información de la política | 2706 |
| Versión de la política | 2706 |
| Documento de política JSON | 2707 |
| Más información | 2707 |
| BatchServiceRolePolicy | 2707 |
| Uso de la política | 2708 |
| Información de la política | 2708 |
| Versión de la política | 2708 |
| Documento de política JSON | 2708 |
| Más información | 2714 |
| Billing | 2714 |
| Uso de la política | 2714 |
| Información de la política | 2715 |
| Versión de la política | 2715 |
| Documento de política JSON | 2715 |
| Más información | 2718 |
| CertificateManagerServiceRolePolicy | 2718 |
| Uso de la política | 2718 |
| Información de la política | 2718 |
| Versión de la política | 2718 |
| Documento de política JSON | 2719 |
| Más información | 2719 |

| | |
|---|------|
| ClientVPNServiceConnectionsRolePolicy | 2719 |
| Uso de la política | 2719 |
| Información de la política | 2719 |
| Versión de la política | 2720 |
| Documento de política JSON | 2720 |
| Más información | 2720 |
| ClientVPNServiceRolePolicy | 2720 |
| Uso de la política | 2721 |
| Información de la política | 2721 |
| Versión de la política | 2721 |
| Documento de política JSON | 2721 |
| Más información | 2722 |
| CloudFormationStackSetsOrgAdminServiceRolePolicy | 2722 |
| Uso de la política | 2722 |
| Información de la política | 2722 |
| Versión de la política | 2723 |
| Documento de política JSON | 2723 |
| Más información | 2723 |
| CloudFormationStackSetsOrgMemberServiceRolePolicy | 2724 |
| Uso de la política | 2724 |
| Información de la política | 2724 |
| Versión de la política | 2724 |
| Documento de política JSON | 2724 |
| Más información | 2725 |
| CloudFrontFullAccess | 2725 |
| Uso de la política | 2725 |
| Información de la política | 2726 |
| Versión de la política | 2726 |
| Documento de política JSON | 2726 |
| Más información | 2727 |
| CloudFrontReadOnlyAccess | 2727 |
| Uso de la política | 2728 |
| Información de la política | 2728 |
| Versión de la política | 2728 |
| Documento de política JSON | 2728 |
| Más información | 2729 |

| | |
|-------------------------------------|------|
| CloudHSMSERVICERolePolicy | 2729 |
| Uso de la política | 2729 |
| Información de la política | 2729 |
| Versión de la política | 2729 |
| Documento de política JSON | 2730 |
| Más información | 2730 |
| CloudSearchFullAccess | 2730 |
| Uso de la política | 2730 |
| Información de la política | 2731 |
| Versión de la política | 2731 |
| Documento de política JSON | 2731 |
| Más información | 2731 |
| CloudSearchReadOnlyAccess | 2732 |
| Uso de la política | 2732 |
| Información de la política | 2732 |
| Versión de la política | 2732 |
| Documento de política JSON | 2732 |
| Más información | 2733 |
| CloudTrailServiceRolePolicy | 2733 |
| Uso de la política | 2733 |
| Información de la política | 2733 |
| Versión de la política | 2733 |
| Documento de política JSON | 2734 |
| Más información | 2735 |
| CloudWatch-CrossAccountAccess | 2735 |
| Uso de la política | 2735 |
| Información de la política | 2736 |
| Versión de la política | 2736 |
| Documento de política JSON | 2736 |
| Más información | 2736 |
| CloudWatchActionsEC2Access | 2737 |
| Uso de la política | 2737 |
| Información de la política | 2737 |
| Versión de la política | 2737 |
| Documento de política JSON | 2737 |
| Más información | 2738 |

| | |
|--|------|
| CloudWatchAgentAdminPolicy | 2738 |
| Uso de la política | 2738 |
| Información de la política | 2738 |
| Versión de la política | 2738 |
| Documento de política JSON | 2739 |
| Más información | 2739 |
| CloudWatchAgentServerPolicy | 2740 |
| Uso de la política | 2740 |
| Información de la política | 2740 |
| Versión de la política | 2740 |
| Documento de política JSON | 2740 |
| Más información | 2741 |
| CloudWatchApplicationInsightsFullAccess | 2741 |
| Uso de la política | 2742 |
| Información de la política | 2742 |
| Versión de la política | 2742 |
| Documento de política JSON | 2742 |
| Más información | 2743 |
| CloudWatchApplicationInsightsReadOnlyAccess | 2744 |
| Uso de la política | 2744 |
| Información de la política | 2744 |
| Versión de la política | 2744 |
| Documento de política JSON | 2744 |
| Más información | 2745 |
| CloudwatchApplicationInsightsServiceLinkedRolePolicy | 2745 |
| Uso de la política | 2745 |
| Información de la política | 2745 |
| Versión de la política | 2745 |
| Documento de política JSON | 2746 |
| Más información | 2755 |
| CloudWatchApplicationSignalsServiceRolePolicy | 2756 |
| Uso de la política | 2756 |
| Información de la política | 2756 |
| Versión de la política | 2756 |
| Documento de política JSON | 2756 |
| Más información | 2758 |

| | |
|--|------|
| CloudWatchAutomaticDashboardsAccess | 2758 |
| Uso de la política | 2758 |
| Información de la política | 2758 |
| Versión de la política | 2759 |
| Documento de política JSON | 2759 |
| Más información | 2760 |
| CloudWatchCrossAccountSharingConfiguration | 2760 |
| Uso de la política | 2761 |
| Información de la política | 2761 |
| Versión de la política | 2761 |
| Documento de política JSON | 2761 |
| Más información | 2762 |
| CloudWatchEventsBuiltInTargetExecutionAccess | 2762 |
| Uso de la política | 2762 |
| Información de la política | 2762 |
| Versión de la política | 2763 |
| Documento de política JSON | 2763 |
| Más información | 2763 |
| CloudWatchEventsFullAccess | 2764 |
| Uso de la política | 2764 |
| Información de la política | 2764 |
| Versión de la política | 2764 |
| Documento de política JSON | 2764 |
| Más información | 2766 |
| CloudWatchEventsInvocationAccess | 2767 |
| Uso de la política | 2767 |
| Información de la política | 2767 |
| Versión de la política | 2767 |
| Documento de política JSON | 2767 |
| Más información | 2768 |
| CloudWatchEventsReadOnlyAccess | 2768 |
| Uso de la política | 2768 |
| Información de la política | 2768 |
| Versión de la política | 2768 |
| Documento de política JSON | 2769 |
| Más información | 2770 |

| | |
|--|------|
| CloudWatchEventsServiceRolePolicy | 2770 |
| Uso de la política | 2770 |
| Información de la política | 2770 |
| Versión de la política | 2771 |
| Documento de política JSON | 2771 |
| Más información | 2771 |
| CloudWatchFullAccess | 2772 |
| Uso de la política | 2772 |
| Información de la política | 2772 |
| Versión de la política | 2772 |
| Documento de política JSON | 2772 |
| Más información | 2773 |
| CloudWatchFullAccessV2 | 2773 |
| Uso de la política | 2774 |
| Información de la política | 2774 |
| Versión de la política | 2774 |
| Documento de política JSON | 2774 |
| Más información | 2776 |
| CloudWatchInternetMonitorServiceRolePolicy | 2776 |
| Uso de la política | 2776 |
| Información de la política | 2776 |
| Versión de la política | 2776 |
| Documento de política JSON | 2777 |
| Más información | 2778 |
| CloudWatchLambdaInsightsExecutionRolePolicy | 2778 |
| Uso de la política | 2778 |
| Información de la política | 2778 |
| Versión de la política | 2778 |
| Documento de política JSON | 2778 |
| Más información | 2779 |
| CloudWatchLogsCrossAccountSharingConfiguration | 2779 |
| Uso de la política | 2779 |
| Información de la política | 2779 |
| Versión de la política | 2780 |
| Documento de política JSON | 2780 |
| Más información | 2781 |

| | |
|---|------|
| CloudWatchLogsFullAccess | 2781 |
| Uso de la política | 2781 |
| Información de la política | 2781 |
| Versión de la política | 2781 |
| Documento de política JSON | 2782 |
| Más información | 2782 |
| CloudWatchLogsReadOnlyAccess | 2782 |
| Uso de la política | 2782 |
| Información de la política | 2783 |
| Versión de la política | 2783 |
| Documento de política JSON | 2783 |
| Más información | 2784 |
| CloudWatchNetworkMonitorServiceRolePolicy | 2784 |
| Uso de la política | 2784 |
| Información de la política | 2784 |
| Versión de la política | 2784 |
| Documento de política JSON | 2785 |
| Más información | 2786 |
| CloudWatchReadOnlyAccess | 2786 |
| Uso de la política | 2786 |
| Información de la política | 2786 |
| Versión de la política | 2786 |
| Documento de política JSON | 2787 |
| Más información | 2788 |
| CloudWatchSyntheticsFullAccess | 2788 |
| Uso de la política | 2788 |
| Información de la política | 2788 |
| Versión de la política | 2789 |
| Documento de política JSON | 2789 |
| Más información | 2793 |
| CloudWatchSyntheticsReadOnlyAccess | 2794 |
| Uso de la política | 2794 |
| Información de la política | 2794 |
| Versión de la política | 2794 |
| Documento de política JSON | 2794 |
| Más información | 2795 |

| | |
|---|------|
| ComprehendDataAccessRolePolicy | 2795 |
| Uso de la política | 2795 |
| Información de la política | 2795 |
| Versión de la política | 2795 |
| Documento de política JSON | 2796 |
| Más información | 2796 |
| ComprehendFullAccess | 2796 |
| Uso de la política | 2796 |
| Información de la política | 2796 |
| Versión de la política | 2797 |
| Documento de política JSON | 2797 |
| Más información | 2797 |
| ComprehendMedicalFullAccess | 2798 |
| Uso de la política | 2798 |
| Información de la política | 2798 |
| Versión de la política | 2798 |
| Documento de política JSON | 2798 |
| Más información | 2799 |
| ComprehendReadOnly | 2799 |
| Uso de la política | 2799 |
| Información de la política | 2799 |
| Versión de la política | 2799 |
| Documento de política JSON | 2800 |
| Más información | 2801 |
| ComputeOptimizerReadOnlyAccess | 2801 |
| Uso de la política | 2801 |
| Información de la política | 2801 |
| Versión de la política | 2802 |
| Documento de política JSON | 2802 |
| Más información | 2803 |
| ComputeOptimizerServiceRolePolicy | 2803 |
| Uso de la política | 2803 |
| Información de la política | 2803 |
| Versión de la política | 2803 |
| Documento de política JSON | 2804 |
| Más información | 2805 |

| | |
|---|------|
| ConfigConformsServiceRolePolicy | 2805 |
| Uso de la política | 2805 |
| Información de la política | 2805 |
| Versión de la política | 2806 |
| Documento de política JSON | 2806 |
| Más información | 2808 |
| CostOptimizationHubAdminAccess | 2809 |
| Uso de la política | 2809 |
| Información de la política | 2809 |
| Versión de la política | 2809 |
| Documento de política JSON | 2809 |
| Más información | 2811 |
| CostOptimizationHubReadOnlyAccess | 2811 |
| Uso de la política | 2811 |
| Información de la política | 2811 |
| Versión de la política | 2811 |
| Documento de política JSON | 2811 |
| Más información | 2812 |
| CostOptimizationHubServiceRolePolicy | 2812 |
| Uso de la política | 2812 |
| Información de la política | 2812 |
| Versión de la política | 2813 |
| Documento de política JSON | 2813 |
| Más información | 2814 |
| CustomerProfilesServiceLinkedRolePolicy | 2814 |
| Uso de la política | 2814 |
| Información de la política | 2814 |
| Versión de la política | 2814 |
| Documento de política JSON | 2815 |
| Más información | 2815 |
| DatabaseAdministrator | 2815 |
| Uso de la política | 2816 |
| Información de la política | 2816 |
| Versión de la política | 2816 |
| Documento de política JSON | 2816 |
| Más información | 2818 |

| | |
|--|------|
| DataScientist | 2819 |
| Uso de la política | 2819 |
| Información de la política | 2819 |
| Versión de la política | 2819 |
| Documento de política JSON | 2819 |
| Más información | 2823 |
| DAXServiceRolePolicy | 2823 |
| Uso de la política | 2823 |
| Información de la política | 2824 |
| Versión de la política | 2824 |
| Documento de política JSON | 2824 |
| Más información | 2825 |
| DynamoDBCloudWatchContributorInsightsServiceRolePolicy | 2825 |
| Uso de la política | 2825 |
| Información de la política | 2825 |
| Versión de la política | 2825 |
| Documento de política JSON | 2825 |
| Más información | 2826 |
| DynamoDBKinesisReplicationServiceRolePolicy | 2826 |
| Uso de la política | 2826 |
| Información de la política | 2826 |
| Versión de la política | 2827 |
| Documento de política JSON | 2827 |
| Más información | 2827 |
| DynamoDBReplicationServiceRolePolicy | 2828 |
| Uso de la política | 2828 |
| Información de la política | 2828 |
| Versión de la política | 2828 |
| Documento de política JSON | 2828 |
| Más información | 2829 |
| EC2FastLaunchServiceRolePolicy | 2830 |
| Uso de la política | 2830 |
| Información de la política | 2830 |
| Versión de la política | 2830 |
| Documento de política JSON | 2830 |
| Más información | 2834 |

| | |
|---|------|
| EC2FleetTimeShiftableServiceRolePolicy | 2834 |
| Uso de la política | 2835 |
| Información de la política | 2835 |
| Versión de la política | 2835 |
| Documento de política JSON | 2835 |
| Más información | 2837 |
| Ec2ImageBuilderCrossAccountDistributionAccess | 2837 |
| Uso de la política | 2837 |
| Información de la política | 2837 |
| Versión de la política | 2837 |
| Documento de política JSON | 2837 |
| Más información | 2838 |
| EC2ImageBuilderLifecycleExecutionPolicy | 2838 |
| Uso de la política | 2838 |
| Información de la política | 2839 |
| Versión de la política | 2839 |
| Documento de política JSON | 2839 |
| Más información | 2841 |
| EC2InstanceConnect | 2841 |
| Uso de la política | 2841 |
| Información de la política | 2841 |
| Versión de la política | 2842 |
| Documento de política JSON | 2842 |
| Más información | 2842 |
| Ec2InstanceConnectEndpoint | 2843 |
| Uso de la política | 2843 |
| Información de la política | 2843 |
| Versión de la política | 2843 |
| Documento de política JSON | 2843 |
| Más información | 2845 |
| EC2InstanceProfileForImageBuilder | 2845 |
| Uso de la política | 2846 |
| Información de la política | 2846 |
| Versión de la política | 2846 |
| Documento de política JSON | 2846 |
| Más información | 2847 |

| | |
|---|------|
| EC2InstanceProfileForImageBuilderECRContainerBuilds | 2847 |
| Uso de la política | 2848 |
| Información de la política | 2848 |
| Versión de la política | 2848 |
| Documento de política JSON | 2848 |
| Más información | 2849 |
| ECRReplicationServiceRolePolicy | 2850 |
| Uso de la política | 2850 |
| Información de la política | 2850 |
| Versión de la política | 2850 |
| Documento de política JSON | 2850 |
| Más información | 2851 |
| ElastiCacheServiceRolePolicy | 2851 |
| Uso de la política | 2851 |
| Información de la política | 2851 |
| Versión de la política | 2851 |
| Documento de política JSON | 2852 |
| Más información | 2854 |
| ElasticLoadBalancingFullAccess | 2854 |
| Uso de la política | 2854 |
| Información de la política | 2854 |
| Versión de la política | 2854 |
| Documento de política JSON | 2854 |
| Más información | 2856 |
| ElasticLoadBalancingReadOnly | 2856 |
| Uso de la política | 2856 |
| Información de la política | 2856 |
| Versión de la política | 2856 |
| Documento de política JSON | 2857 |
| Más información | 2858 |
| ElementalActivationsDownloadSoftwareAccess | 2858 |
| Uso de la política | 2858 |
| Información de la política | 2858 |
| Versión de la política | 2858 |
| Documento de política JSON | 2859 |
| Más información | 2859 |

| | |
|---|------|
| ElementalActivationsFullAccess | 2859 |
| Uso de la política | 2859 |
| Información de la política | 2859 |
| Versión de la política | 2860 |
| Documento de política JSON | 2860 |
| Más información | 2860 |
| ElementalActivationsGenerateLicenses | 2861 |
| Uso de la política | 2861 |
| Información de la política | 2861 |
| Versión de la política | 2861 |
| Documento de política JSON | 2861 |
| Más información | 2862 |
| ElementalActivationsReadOnlyAccess | 2862 |
| Uso de la política | 2862 |
| Información de la política | 2862 |
| Versión de la política | 2862 |
| Documento de política JSON | 2863 |
| Más información | 2863 |
| ElementalAppliancesSoftwareFullAccess | 2863 |
| Uso de la política | 2863 |
| Información de la política | 2863 |
| Versión de la política | 2864 |
| Documento de política JSON | 2864 |
| Más información | 2864 |
| ElementalAppliancesSoftwareReadOnlyAccess | 2865 |
| Uso de la política | 2865 |
| Información de la política | 2865 |
| Versión de la política | 2865 |
| Documento de política JSON | 2865 |
| Más información | 2866 |
| ElementalSupportCenterFullAccess | 2866 |
| Uso de la política | 2866 |
| Información de la política | 2866 |
| Versión de la política | 2866 |
| Documento de política JSON | 2867 |
| Más información | 2867 |

| | |
|---|------|
| EMRDescribeClusterPolicyForEMRWAL | 2867 |
| Uso de la política | 2867 |
| Información de la política | 2868 |
| Versión de la política | 2868 |
| Documento de política JSON | 2868 |
| Más información | 2868 |
| FMSServiceRolePolicy | 2869 |
| Uso de la política | 2869 |
| Información de la política | 2869 |
| Versión de la política | 2869 |
| Documento de política JSON | 2869 |
| Más información | 2883 |
| FSxDeleteServiceLinkedRoleAccess | 2883 |
| Uso de la política | 2884 |
| Información de la política | 2884 |
| Versión de la política | 2884 |
| Documento de política JSON | 2884 |
| Más información | 2885 |
| GameLiftGameServerGroupPolicy | 2885 |
| Uso de la política | 2885 |
| Información de la política | 2885 |
| Versión de la política | 2885 |
| Documento de política JSON | 2885 |
| Más información | 2887 |
| GlobalAcceleratorFullAccess | 2887 |
| Uso de la política | 2887 |
| Información de la política | 2887 |
| Versión de la política | 2888 |
| Documento de política JSON | 2888 |
| Más información | 2889 |
| GlobalAcceleratorReadOnlyAccess | 2889 |
| Uso de la política | 2889 |
| Información de la política | 2889 |
| Versión de la política | 2890 |
| Documento de política JSON | 2890 |
| Más información | 2890 |

| | |
|---|------|
| GreengrassOTAUpdateArtifactAccess | 2890 |
| Uso de la política | 2891 |
| Información de la política | 2891 |
| Versión de la política | 2891 |
| Documento de política JSON | 2891 |
| Más información | 2892 |
| GroundTruthSyntheticConsoleFullAccess | 2892 |
| Uso de la política | 2892 |
| Información de la política | 2892 |
| Versión de la política | 2892 |
| Documento de política JSON | 2892 |
| Más información | 2893 |
| GroundTruthSyntheticConsoleReadOnlyAccess | 2893 |
| Uso de la política | 2893 |
| Información de la política | 2893 |
| Versión de la política | 2894 |
| Documento de política JSON | 2894 |
| Más información | 2894 |
| Health_OrganizationsServiceRolePolicy | 2894 |
| Uso de la política | 2895 |
| Información de la política | 2895 |
| Versión de la política | 2895 |
| Documento de política JSON | 2895 |
| Más información | 2896 |
| IAMAccessAdvisorReadOnly | 2896 |
| Uso de la política | 2896 |
| Información de la política | 2896 |
| Versión de la política | 2896 |
| Documento de política JSON | 2896 |
| Más información | 2897 |
| IAMAccessAnalyzerFullAccess | 2898 |
| Uso de la política | 2898 |
| Información de la política | 2898 |
| Versión de la política | 2898 |
| Documento de política JSON | 2898 |
| Más información | 2899 |

| | |
|---|------|
| IAMAccessAnalyzerReadOnlyAccess | 2899 |
| Uso de la política | 2900 |
| Información de la política | 2900 |
| Versión de la política | 2900 |
| Documento de política JSON | 2900 |
| Más información | 2901 |
| IAMFullAccess | 2901 |
| Uso de la política | 2901 |
| Información de la política | 2901 |
| Versión de la política | 2901 |
| Documento de política JSON | 2901 |
| Más información | 2902 |
| IAMReadOnlyAccess | 2902 |
| Uso de la política | 2902 |
| Información de la política | 2903 |
| Versión de la política | 2903 |
| Documento de política JSON | 2903 |
| Más información | 2903 |
| IAMSelfManageServiceSpecificCredentials | 2904 |
| Uso de la política | 2904 |
| Información de la política | 2904 |
| Versión de la política | 2904 |
| Documento de política JSON | 2904 |
| Más información | 2905 |
| IAMUserChangePassword | 2905 |
| Uso de la política | 2905 |
| Información de la política | 2905 |
| Versión de la política | 2906 |
| Documento de política JSON | 2906 |
| Más información | 2906 |
| IAMUserSSHKeys | 2907 |
| Uso de la política | 2907 |
| Información de la política | 2907 |
| Versión de la política | 2907 |
| Documento de política JSON | 2907 |
| Más información | 2908 |

| | |
|---|------|
| IVSFullAccess | 2908 |
| Uso de la política | 2908 |
| Información de la política | 2908 |
| Versión de la política | 2908 |
| Documento de política JSON | 2909 |
| Más información | 2909 |
| IVSReadOnlyAccess | 2909 |
| Uso de la política | 2909 |
| Información de la política | 2909 |
| Versión de la política | 2910 |
| Documento de política JSON | 2910 |
| Más información | 2911 |
| IVSRecordToS3 | 2911 |
| Uso de la política | 2911 |
| Información de la política | 2911 |
| Versión de la política | 2912 |
| Documento de política JSON | 2912 |
| Más información | 2912 |
| KafkaConnectServiceRolePolicy | 2912 |
| Uso de la política | 2913 |
| Información de la política | 2913 |
| Versión de la política | 2913 |
| Documento de política JSON | 2913 |
| Más información | 2915 |
| KafkaServiceRolePolicy | 2915 |
| Uso de la política | 2915 |
| Información de la política | 2915 |
| Versión de la política | 2915 |
| Documento de política JSON | 2915 |
| Más información | 2917 |
| KeyspacesReplicationServiceRolePolicy | 2917 |
| Uso de la política | 2917 |
| Información de la política | 2917 |
| Versión de la política | 2917 |
| Documento de política JSON | 2918 |
| Más información | 2918 |

| | |
|--|------|
| LakeFormationDataAccessServiceRolePolicy | 2918 |
| Uso de la política | 2918 |
| Información de la política | 2919 |
| Versión de la política | 2919 |
| Documento de política JSON | 2919 |
| Más información | 2919 |
| LexBotPolicy | 2920 |
| Uso de la política | 2920 |
| Información de la política | 2920 |
| Versión de la política | 2920 |
| Documento de política JSON | 2920 |
| Más información | 2921 |
| LexChannelPolicy | 2921 |
| Uso de la política | 2921 |
| Información de la política | 2921 |
| Versión de la política | 2921 |
| Documento de política JSON | 2922 |
| Más información | 2922 |
| LightsailExportAccess | 2922 |
| Uso de la política | 2922 |
| Información de la política | 2922 |
| Versión de la política | 2923 |
| Documento de política JSON | 2923 |
| Más información | 2924 |
| MediaConnectGatewayInstanceRolePolicy | 2924 |
| Uso de la política | 2924 |
| Información de la política | 2924 |
| Versión de la política | 2924 |
| Documento de política JSON | 2924 |
| Más información | 2925 |
| MediaPackageServiceRolePolicy | 2925 |
| Uso de la política | 2925 |
| Información de la política | 2925 |
| Versión de la política | 2926 |
| Documento de política JSON | 2926 |
| Más información | 2926 |

| | |
|--|------|
| MemoryDBServiceRolePolicy | 2927 |
| Uso de la política | 2927 |
| Información de la política | 2927 |
| Versión de la política | 2927 |
| Documento de política JSON | 2927 |
| Más información | 2929 |
| MigrationHubDMSAccessServiceRolePolicy | 2929 |
| Uso de la política | 2929 |
| Información de la política | 2929 |
| Versión de la política | 2930 |
| Documento de política JSON | 2930 |
| Más información | 2931 |
| MigrationHubServiceRolePolicy | 2931 |
| Uso de la política | 2931 |
| Información de la política | 2931 |
| Versión de la política | 2931 |
| Documento de política JSON | 2932 |
| Más información | 2933 |
| MigrationHubSMSAccessServiceRolePolicy | 2933 |
| Uso de la política | 2933 |
| Información de la política | 2933 |
| Versión de la política | 2934 |
| Documento de política JSON | 2934 |
| Más información | 2935 |
| MonitronServiceRolePolicy | 2935 |
| Uso de la política | 2935 |
| Información de la política | 2935 |
| Versión de la política | 2935 |
| Documento de política JSON | 2935 |
| Más información | 2936 |
| NeptuneConsoleFullAccess | 2936 |
| Uso de la política | 2936 |
| Información de la política | 2936 |
| Versión de la política | 2937 |
| Documento de política JSON | 2937 |
| Más información | 2942 |

| | |
|----------------------------------|------|
| NeptuneFullAccess | 2943 |
| Uso de la política | 2943 |
| Información de la política | 2943 |
| Versión de la política | 2943 |
| Documento de política JSON | 2943 |
| Más información | 2947 |
| NeptuneGraphReadOnlyAccess | 2947 |
| Uso de la política | 2948 |
| Información de la política | 2948 |
| Versión de la política | 2948 |
| Documento de política JSON | 2948 |
| Más información | 2950 |
| NeptuneReadOnlyAccess | 2950 |
| Uso de la política | 2950 |
| Información de la política | 2950 |
| Versión de la política | 2950 |
| Documento de política JSON | 2951 |
| Más información | 2953 |
| NetworkAdministrator | 2953 |
| Uso de la política | 2953 |
| Información de la política | 2953 |
| Versión de la política | 2953 |
| Documento de política JSON | 2954 |
| Más información | 2960 |
| OAMFullAccess | 2960 |
| Uso de la política | 2961 |
| Información de la política | 2961 |
| Versión de la política | 2961 |
| Documento de política JSON | 2961 |
| Más información | 2961 |
| OAMReadOnlyAccess | 2962 |
| Uso de la política | 2962 |
| Información de la política | 2962 |
| Versión de la política | 2962 |
| Documento de política JSON | 2962 |
| Más información | 2963 |

| | |
|---|------|
| PartnerCentralAccountManagementUserRoleAssociation | 2963 |
| Uso de la política | 2963 |
| Información de la política | 2963 |
| Versión de la política | 2963 |
| Documento de política JSON | 2964 |
| Más información | 2964 |
| PowerUserAccess | 2965 |
| Uso de la política | 2965 |
| Información de la política | 2965 |
| Versión de la política | 2965 |
| Documento de política JSON | 2965 |
| Más información | 2966 |
| QuickSightAccessForS3StorageManagementAnalyticsReadOnly | 2966 |
| Uso de la política | 2966 |
| Información de la política | 2967 |
| Versión de la política | 2967 |
| Documento de política JSON | 2967 |
| Más información | 2968 |
| RDSCloudHsmAuthorizationRole | 2968 |
| Uso de la política | 2968 |
| Información de la política | 2968 |
| Versión de la política | 2968 |
| Documento de política JSON | 2969 |
| Más información | 2969 |
| ReadOnlyAccess | 2969 |
| Uso de la política | 2969 |
| Información de la política | 2970 |
| Versión de la política | 2970 |
| Documento de política JSON | 2970 |
| Más información | 3016 |
| ResourceGroupsandTagEditorFullAccess | 3017 |
| Uso de la política | 3017 |
| Información de la política | 3017 |
| Versión de la política | 3017 |
| Documento de política JSON | 3017 |
| Más información | 3018 |

| | |
|--|------|
| ResourceGroupsandTagEditorReadOnlyAccess | 3018 |
| Uso de la política | 3018 |
| Información de la política | 3018 |
| Versión de la política | 3018 |
| Documento de política JSON | 3019 |
| Más información | 3019 |
| ResourceGroupsServiceRolePolicy | 3020 |
| Uso de la política | 3020 |
| Información de la política | 3020 |
| Versión de la política | 3020 |
| Documento de política JSON | 3020 |
| Más información | 3021 |
| ROSAAmazonEBSCSIDriverOperatorPolicy | 3021 |
| Uso de la política | 3021 |
| Información de la política | 3021 |
| Versión de la política | 3021 |
| Documento de política JSON | 3022 |
| Más información | 3025 |
| ROSACloudNetworkConfigOperatorPolicy | 3025 |
| Uso de la política | 3025 |
| Información de la política | 3025 |
| Versión de la política | 3025 |
| Documento de política JSON | 3026 |
| Más información | 3027 |
| ROSAControlPlaneOperatorPolicy | 3027 |
| Uso de la política | 3027 |
| Información de la política | 3027 |
| Versión de la política | 3027 |
| Documento de política JSON | 3027 |
| Más información | 3032 |
| ROSAImageRegistryOperatorPolicy | 3032 |
| Uso de la política | 3032 |
| Información de la política | 3032 |
| Versión de la política | 3033 |
| Documento de política JSON | 3033 |
| Más información | 3034 |

| | |
|------------------------------------|------|
| ROSAIngressOperatorPolicy | 3034 |
| Uso de la política | 3035 |
| Información de la política | 3035 |
| Versión de la política | 3035 |
| Documento de política JSON | 3035 |
| Más información | 3036 |
| ROSAInstallerPolicy | 3036 |
| Uso de la política | 3036 |
| Información de la política | 3036 |
| Versión de la política | 3037 |
| Documento de política JSON | 3037 |
| Más información | 3044 |
| ROSAKMSProviderPolicy | 3044 |
| Uso de la política | 3044 |
| Información de la política | 3044 |
| Versión de la política | 3045 |
| Documento de política JSON | 3045 |
| Más información | 3045 |
| ROSAKubeControllerPolicy | 3046 |
| Uso de la política | 3046 |
| Información de la política | 3046 |
| Versión de la política | 3046 |
| Documento de política JSON | 3046 |
| Más información | 3051 |
| ROSAManageSubscription | 3051 |
| Uso de la política | 3051 |
| Información de la política | 3051 |
| Versión de la política | 3051 |
| Documento de política JSON | 3052 |
| Más información | 3052 |
| ROSANodePoolManagementPolicy | 3053 |
| Uso de la política | 3053 |
| Información de la política | 3053 |
| Versión de la política | 3053 |
| Documento de política JSON | 3053 |
| Más información | 3059 |

| | |
|---|------|
| ROSASRESupportPolicy | 3059 |
| Uso de la política | 3059 |
| Información de la política | 3059 |
| Versión de la política | 3060 |
| Documento de política JSON | 3060 |
| Más información | 3065 |
| ROSAWorkerInstancePolicy | 3065 |
| Uso de la política | 3065 |
| Información de la política | 3065 |
| Versión de la política | 3065 |
| Documento de política JSON | 3066 |
| Más información | 3066 |
| Route53RecoveryReadinessServiceRolePolicy | 3066 |
| Uso de la política | 3066 |
| Información de la política | 3066 |
| Versión de la política | 3067 |
| Documento de política JSON | 3067 |
| Más información | 3070 |
| Route53ResolverServiceRolePolicy | 3071 |
| Uso de la política | 3071 |
| Información de la política | 3071 |
| Versión de la política | 3071 |
| Documento de política JSON | 3071 |
| Más información | 3072 |
| S3StorageLensServiceRolePolicy | 3072 |
| Uso de la política | 3072 |
| Información de la política | 3072 |
| Versión de la política | 3072 |
| Documento de política JSON | 3073 |
| Más información | 3073 |
| SecretsManagerReadWrite | 3073 |
| Uso de la política | 3074 |
| Información de la política | 3074 |
| Versión de la política | 3074 |
| Documento de política JSON | 3074 |
| Más información | 3076 |

| | |
|---|------|
| SecurityAudit | 3076 |
| Uso de la política | 3076 |
| Información de la política | 3076 |
| Versión de la política | 3076 |
| Documento de política JSON | 3077 |
| Más información | 3092 |
| SecurityLakeServiceLinkedRole | 3092 |
| Uso de la política | 3093 |
| Información de la política | 3093 |
| Versión de la política | 3093 |
| Documento de política JSON | 3093 |
| Más información | 3096 |
| ServerMigration_ServiceRole | 3096 |
| Uso de la política | 3096 |
| Información de la política | 3096 |
| Versión de la política | 3096 |
| Documento de política JSON | 3096 |
| Más información | 3101 |
| ServerMigrationConnector | 3101 |
| Uso de la política | 3102 |
| Información de la política | 3102 |
| Versión de la política | 3102 |
| Documento de política JSON | 3102 |
| Más información | 3104 |
| ServerMigrationServiceConsoleFullAccess | 3104 |
| Uso de la política | 3104 |
| Información de la política | 3104 |
| Versión de la política | 3104 |
| Documento de política JSON | 3104 |
| Más información | 3106 |
| ServerMigrationServiceLaunchRole | 3106 |
| Uso de la política | 3106 |
| Información de la política | 3107 |
| Versión de la política | 3107 |
| Documento de política JSON | 3107 |
| Más información | 3110 |

| | |
|---|------|
| ServerMigrationServiceRoleForInstanceValidation | 3110 |
| Uso de la política | 3110 |
| Información de la política | 3110 |
| Versión de la política | 3110 |
| Documento de política JSON | 3111 |
| Más información | 3111 |
| ServiceQuotasFullAccess | 3111 |
| Uso de la política | 3111 |
| Información de la política | 3112 |
| Versión de la política | 3112 |
| Documento de política JSON | 3112 |
| Más información | 3114 |
| ServiceQuotasReadOnlyAccess | 3114 |
| Uso de la política | 3114 |
| Información de la política | 3114 |
| Versión de la política | 3114 |
| Documento de política JSON | 3115 |
| Más información | 3116 |
| ServiceQuotasServiceRolePolicy | 3116 |
| Uso de la política | 3116 |
| Información de la política | 3116 |
| Versión de la política | 3116 |
| Documento de política JSON | 3117 |
| Más información | 3117 |
| SimpleWorkflowFullAccess | 3117 |
| Uso de la política | 3117 |
| Información de la política | 3117 |
| Versión de la política | 3118 |
| Documento de política JSON | 3118 |
| Más información | 3118 |
| SupportUser | 3118 |
| Uso de la política | 3119 |
| Información de la política | 3119 |
| Versión de la política | 3119 |
| Documento de política JSON | 3119 |
| Más información | 3124 |

| | |
|---|------|
| SystemAdministrator | 3124 |
| Uso de la política | 3124 |
| Información de la política | 3124 |
| Versión de la política | 3125 |
| Documento de política JSON | 3125 |
| Más información | 3131 |
| TranslateFullAccess | 3131 |
| Uso de la política | 3131 |
| Información de la política | 3131 |
| Versión de la política | 3131 |
| Documento de política JSON | 3132 |
| Más información | 3132 |
| TranslateReadOnly | 3133 |
| Uso de la política | 3133 |
| Información de la política | 3133 |
| Versión de la política | 3133 |
| Documento de política JSON | 3133 |
| Más información | 3134 |
| ViewOnlyAccess | 3134 |
| Uso de la política | 3134 |
| Información de la política | 3134 |
| Versión de la política | 3134 |
| Documento de política JSON | 3135 |
| Más información | 3140 |
| VMImportExportRoleForAWSConnector | 3141 |
| Uso de la política | 3141 |
| Información de la política | 3141 |
| Versión de la política | 3141 |
| Documento de política JSON | 3141 |
| Más información | 3142 |
| VPCLatticeFullAccess | 3142 |
| Uso de la política | 3143 |
| Información de la política | 3143 |
| Versión de la política | 3143 |
| Documento de política JSON | 3143 |
| Más información | 3145 |

| | |
|---|------|
| VPCLatticeReadOnlyAccess | 3145 |
| Uso de la política | 3145 |
| Información de la política | 3146 |
| Versión de la política | 3146 |
| Documento de política JSON | 3146 |
| Más información | 3147 |
| VPCLatticeServicesInvokeAccess | 3147 |
| Uso de la política | 3147 |
| Información de la política | 3147 |
| Versión de la política | 3147 |
| Documento de política JSON | 3148 |
| Más información | 3148 |
| WAFLoggingServiceRolePolicy | 3148 |
| Uso de la política | 3148 |
| Información de la política | 3149 |
| Versión de la política | 3149 |
| Documento de política JSON | 3149 |
| Más información | 3149 |
| WAFRegionalLoggingServiceRolePolicy | 3150 |
| Uso de la política | 3150 |
| Información de la política | 3150 |
| Versión de la política | 3150 |
| Documento de política JSON | 3150 |
| Más información | 3151 |
| WAFV2LoggingServiceRolePolicy | 3151 |
| Uso de la política | 3151 |
| Información de la política | 3151 |
| Versión de la política | 3151 |
| Documento de política JSON | 3152 |
| Más información | 3152 |
| WellArchitectedConsoleFullAccess | 3152 |
| Uso de la política | 3152 |
| Información de la política | 3153 |
| Versión de la política | 3153 |
| Documento de política JSON | 3153 |
| Más información | 3153 |

| | |
|--|----------|
| WellArchitectedConsoleReadOnlyAccess | 3154 |
| Uso de la política | 3154 |
| Información de la política | 3154 |
| Versión de la política | 3154 |
| Documento de política JSON | 3154 |
| Más información | 3155 |
| WorkLinkServiceRolePolicy | 3155 |
| Uso de la política | 3155 |
| Información de la política | 3155 |
| Versión de la política | 3155 |
| Documento de política JSON | 3156 |
| Más información | 3156 |
| | mmmcivii |

¿Qué son las políticas administradas por AWS?

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes. Podrá comenzar a asignar de forma más sencilla los permisos adecuados a los usuarios, grupos y roles que si tuviera que escribir políticas.

Tenga presente que es posible que las políticas administradas de AWS no concedan permisos de privilegios mínimos para sus casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir [políticas administradas por el cliente](#) para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas de AWS. Si AWS actualiza los permisos definidos en un política administrada de AWS, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo servicio AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte [políticas administradas de AWS](#) en la Guía del usuario de IAM.

Descripción de las páginas de referencia de las políticas

Cada página de referencia de las políticas incluye la siguiente información:

- Uso de esta política : si puede adjuntar la política a usuarios, grupos y roles
- Detalles de la política
 - Tipo: el tipo de política administrada de AWS
 - `AWS managed policy`: una política administrada estándar de AWS
 - `Job function policy`: política que se alinea con las funciones laborales comunes de la industria
 - `Service-linked role policy`: política que se adjunta a un rol vinculado a servicios que permite a un servicio realizar acciones en su nombre, como [the section called “AmazonRDSPreviewServiceRolePolicy”](#)
 - `Service role policy`: política diseñada para trabajar con roles de servicio, como [the section called “AWSControlTowerServiceRolePolicy”](#)

- Hora de creación: cuándo se creó la política por primera vez
- Hora de edición: cuándo se editó esta versión de la política
- ARN: nombre de recurso de Amazon de la política
- Versión de la política: la versión de los permisos otorgados por la política
- Documento de política de JSON: la política de JSON
- Más información: enlaces a la documentación relacionada con las políticas administradas de AWS

Políticas obsoletas administradas por AWS

AWS actualiza las políticas administradas de AWS de forma periódica. En la mayoría de los casos, agregamos permisos a una política. Esto sucede cuando lanzamos un nuevo servicio o característica. Para mejorar la seguridad de las políticas administradas de AWS, a veces reducimos el alcance de las políticas. Cuando eliminamos los permisos de una política, determinamos el estado obsoleto de la política y ponemos a disposición una nueva. Cuando AWS descarta un servicio o una característica, también descartamos la política administrada AWS para esa característica.

Si recibe una notificación por correo electrónico en la que se indica que una política que está utilizando está descartada, le recomendamos que tome medidas de inmediato. Identifique el cambio en la política y actualice sus flujos de trabajo. Si AWS proporciona una política de reemplazo, planea adjuntarla a todas las identidades afectadas (usuarios, grupos y roles) y luego separe la política obsoleta de esas identidades.

Una política descartada tiene las siguientes características:

- Se ha eliminado de esta guía.
- Los permisos siguen funcionando para todas las identidades asociadas actualmente.
- En las cuentas donde la política está adjunta a una identidad, aparece en la lista de Políticas de la consola de IAM con un icono de advertencia al lado.
- No se puede adjuntar a ninguna identidad nueva. Si la separa de una identidad actual, no puede volver a acoplarla.
- Después de separarla de todas las entidades actuales, ya no es visible.

AWS políticas gestionadas

AWS políticas gestionadas

- [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](#)
- [AmazonEKSFargateServiceRolePolicy](#)
- [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](#)

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

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

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

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

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

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

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

- [AWSIoTDeviceTesterForFreeRTOSFullAccess](#)
- [AWSIoTDeviceTesterForGreengrassFullAccess](#)
- [AWSIoTEventsFullAccess](#)
- [AWSIoTEventsReadOnlyAccess](#)
- [AWSIoTFleetHubFederationAccess](#)
- [AWSIoTFleetwiseServiceRolePolicy](#)
- [AWSIoTFullAccess](#)
- [AWSIoTLogging](#)
- [AWSIoTOTAUpdate](#)
- [AWSIoTRoboRunnerFullAccess](#)
- [AWSIoTRoboRunnerReadOnly](#)
- [AWSIoTRoboRunnerServiceRolePolicy](#)
- [AWSIoTRuleActions](#)
- [AWSIoTSiteWiseConsoleFullAccess](#)
- [AWSIoTSiteWiseFullAccess](#)
- [AWSIoTSiteWiseMonitorPortalAccess](#)
- [AWSIoTSiteWiseMonitorServiceRolePolicy](#)
- [AWSIoTSiteWiseReadOnlyAccess](#)
- [AWSIoTThingsRegistration](#)
- [AWSIoTTwinMakerServiceRolePolicy](#)
- [AWSIoTWirelessDataAccess](#)
- [AWSIoTWirelessFullAccess](#)
- [AWSIoTWirelessFullPublishAccess](#)
- [AWSIoTWirelessGatewayCertManager](#)
- [AWSIoTWirelessLogging](#)
- [AWSIoTWirelessReadOnlyAccess](#)
- [AWSIPAMServiceRolePolicy](#)
- [AWSIQContractServiceRolePolicy](#)
- [AWSIQFullAccess](#)
- [AWSIQPermissionServiceRolePolicy](#)

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

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

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

- [AWSPriceListServiceFullAccess](#)
- [AWSPprivateCAAuditor](#)
- [AWSPprivateCAFullAccess](#)
- [AWSPprivateCAPrivilegedUser](#)
- [AWSPprivateCARedOnly](#)
- [AWSPprivateCAUser](#)
- [AWSPprivateMarketplaceAdminFullAccess](#)
- [AWSPprivateMarketplaceRequests](#)
- [AWSPprivateNetworksServiceRolePolicy](#)
- [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](#)
- [AWSServiceRoleForCloudWatchAlarmsActionSSMSserviceRolePolicy](#)
- [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](#)
- [AWSSStepFunctionsConsoleFullAccess](#)
- [AWSSStepFunctionsFullAccess](#)

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

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

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

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

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

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

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

- [ViewOnlyAccess](#)
- [VMImportExportRoleForAWSConnector](#)
- [VPC_LatticeFullAccess](#)
- [VPC_LatticeReadOnlyAccess](#)
- [VPC_LatticeServicesInvokeAccess](#)
- [WAFLoggingServiceRolePolicy](#)
- [WAFRegionalLoggingServiceRolePolicy](#)
- [WAFV2LoggingServiceRolePolicy](#)
- [WellArchitectedConsoleFullAccess](#)
- [WellArchitectedConsoleReadOnlyAccess](#)
- [WorkLinkServiceRolePolicy](#)

AccessAnalyzerServiceRolePolicy

AccessAnalyzerServiceRolePolicy es una [política administrada AWS](#) que: permite el análisis de los metadatos del recurso por parte del analizador de acceso

Uso de esta política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de diciembre de 2019 a las 17:13 UTC
- Hora editada: 22 de enero de 2024, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Versión de la política

Versión de la política: v12 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AdministratorAccess

AdministratorAccesses una [política AWS gestionada](#) que: proporciona acceso total a AWS los servicios y recursos.

Uso de la política

Puede asociar AdministratorAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AdministratorAccess-Amplify

AdministratorAccess-Amplify es una [política administrada por AWS](#) que: otorga permisos administrativos a las cuentas y, al mismo tiempo, permite explícitamente el acceso directo a los recursos que necesitan las aplicaciones de Amplify.

Uso de esta política

Puede asociar AdministratorAccess-Amplify a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2020 a las 19:03 UTC
- Hora de edición: 31 de mayo de 2023 a las 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CLICloudformationPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation>DeleteStackSet",
        "cloudformation:DescribeStackSet",
        "cloudformation:UpdateStackSet"
      ]
    }
  ]
}
```

```
    ],
    "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:AdminListGroupsWithUser",
    "cognito-idp:ListGroupsWithUser",
    "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:*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AdministratorAccess-AWSElasticBeanstalk

AdministratorAccess-AWSElasticBeanstalk es una [política administrada por AWS](#) que: concede permisos administrativos a la cuenta. Permite explícitamente a los desarrolladores y administradores obtener acceso directo a los recursos que necesitan para administrar las aplicaciones de Elastic Beanstalk AWS

Uso de esta política

Puede asociar AdministratorAccess-AWSElasticBeanstalk a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de enero de 2021 a las 19:36 UTC
- Hora de edición: 23 de marzo de 2023 a las 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

```

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

```

```

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

```

```

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

```



```
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:AddRoleToInstanceProfile",
    "iam:CreateInstanceProfile",
    "iam:CreateRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-elasticbeanstalk*",
    "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:AttachRolePolicy"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
  "Condition" : {
    "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"
      ]
    }
  }
}
]
}
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AlexaForBusinessDeviceSetup

AlexaForBusinessDeviceSetup es una [política administrada por AWS](#) que: proporciona acceso a la configuración del dispositivo a los servicios de AlexaForBusiness

Uso de esta política

Puede asociar AlexaForBusinessDeviceSetup a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2017 a las 16:47 UTC
- Hora de edición: 20 de mayo de 2019 a las 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AlexaForBusinessFullAccess

AlexaForBusinessFullAccess es una [política administrada por AWS](#) que: otorga acceso total a los recursos de AlexaForBusiness y acceso a los Servicios de AWS relacionados

Uso de esta política

Puede asociar AlexaForBusinessFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 30 de noviembre de 2017 a las 16:47 UTC
- Hora de edición: 1 de julio de 2020 a las 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AlexaForBusinessGatewayExecution

AlexaForBusinessGatewayExecution es una [política administrada por AWS](#) que: proporciona acceso de ejecución mediante puerta de enlace a los servicios de AlexaForBusiness

Uso de esta política

Puede asociar AlexaForBusinessGatewayExecution a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2017 a las 16:47 UTC
- Hora de edición: 30 de noviembre de 2017 a las 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

AlexaForBusinessLifesizeDelegatedAccessPolicy es una [política administrada por AWS](#) que: proporciona acceso a los dispositivos AVS de Lifesize

Uso de esta política

Puede asociar AlexaForBusinessLifesizeDelegatedAccessPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de junio de 2020 a las 19:46 UTC
- Hora de edición: 12 de junio de 2020 a las 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    ],
    "Condition" : {
      "StringEquals" : {
        "a4b:amazonId" : [
          "A2IW07UEGWV4TL"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:SearchDevices"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAllValues:StringLike" : {
        "a4b:filters_deviceType" : [
          "*A2IW07UEGWV4TL"
        ]
      },
      "Null" : {
        "a4b:filters_deviceType" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:AssociateDeviceWithRoom"
    ],
    "Resource" : [
      "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGWV4TL",
      "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/*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AlexaForBusinessNetworkProfileServicePolicy

AlexaForBusinessNetworkProfileServicePolicy es una [política administrada por AWS](#) que: permite a Alexa for Business realizar tareas automatizadas programadas por los perfiles de red.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de marzo de 2019 a las 00:53 UTC
- Hora de edición: 5 de abril de 2019 a las 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "A4bPcaTagAccess",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate",
        "acm-pca:RevokeCertificate"
      ],
      "Effect" : "Allow",
```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/a4b" : "enabled"
      }
    },
    {
      "Sid" : "A4bNetworkProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AlexaForBusinessPolyDelegatedAccessPolicy

AlexaForBusinessPolyDelegatedAccessPolicy es una [política administrada por AWS](#) que proporciona acceso a los dispositivos Poly AVS

Uso de esta política

Puede asociar AlexaForBusinessPolyDelegatedAccessPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 16 de octubre de 2019 a las 19:48 UTC
- Hora de edición: 16 de octubre de 2019 a las 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AlexaForBusinessReadOnlyAccess

AlexaForBusinessReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a los servicios de AlexaForBusiness

Uso de esta política

Puede asociar AlexaForBusinessReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2017 a las 16:47 UTC
- Hora de edición: 20 de noviembre de 2019 a las 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAPIGatewayAdministrator

AmazonAPIGatewayAdministrator es una [política administrada por AWS](#) que: proporciona acceso total para crear, editar o eliminar API en Amazon API Gateway a través de AWS Management Console

Uso de esta política

Puede asociar AmazonAPIGatewayAdministrator a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de julio de 2015 a las 17:34 UTC
- Hora de edición: 9 de julio de 2015 a las 17:34 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAPIGatewayInvokeFullAccess

AmazonAPIGatewayInvokeFullAccess es una [política administrada por AWS](#) que: proporciona acceso total para invocar las API en Amazon API Gateway.

Uso de esta política

Puede asociar `AmazonAPIGatewayInvokeFullAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de julio de 2015 a las 17:36 UTC
- Hora de edición: 18 de diciembre de 2018 a las 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAPIGatewayPushToCloudWatchLogs

AmazonAPIGatewayPushToCloudWatchLogs es una [política administrada por AWS](#) que: permite a API Gateway enviar registros a la cuenta del usuario.

Uso de esta política

Puede asociar AmazonAPIGatewayPushToCloudWatchLogs a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de noviembre de 2015 a las 23:41 UTC
- Hora de edición: 11 de noviembre de 2015 a las 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAppFlowFullAccess

AmazonAppFlowFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon AppFlow y acceso a los servicios compatibles AWS como origen o destino del flujo (S3 y Redshift). También proporciona acceso a KMS para el cifrado

Uso de esta política

Puede asociar AmazonAppFlowFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de junio de 2020 a las 23:30 UTC
- Hora de edición: 28 de febrero de 2022 a las 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```

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

```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAppFlowReadOnlyAccess

AmazonAppFlowReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a los flujos de Amazon Appflow

Uso de esta política

Puede asociar AmazonAppFlowReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de junio de 2020 a las 23:26 UTC
- Hora de edición: 28 de febrero de 2022 a las 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "appflow:DescribeConnector",
      "appflow:DescribeConnectors",
      "appflow:DescribeConnectorProfiles",
      "appflow:DescribeFlows",
      "appflow:DescribeFlowExecution",
      "appflow:DescribeConnectorFields",
      "appflow:ListConnectors",
      "appflow:ListConnectorFields",
      "appflow:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAppStreamFullAccess

AmazonAppStreamFullAccess es una [política AWS gestionada](#) que: proporciona acceso total a Amazon AppStream a través de. AWS Management Console

Uso de esta política

Puede asociar AmazonAppStreamFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 28 de agosto de 2020 a las 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

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

```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAppStreamPCAAccess

AmazonAppStreamPCAAccess es una [política administrada por AWS](#) que: permite a Amazon AppStream 2.0 acceso a Certificate Manager Private CA AWS en las cuentas de los clientes para la autenticación basada en certificados

Uso de esta política

Puede asociar AmazonAppStreamPCAAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de octubre de 2022 a las 17:05 UTC
- Hora de edición: 24 de octubre de 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAppStreamReadOnlyAccess

AmazonAppStreamReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon AppStream a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonAppStreamReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 7 de diciembre de 2016 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAppStreamServiceAccess

AmazonAppStreamServiceAccess es una [política administrada por AWS](#) que se encuentra predeterminada para el rol de servicio Amazon AppStream.

Uso de esta política

Puede asociar AmazonAppStreamServiceAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de noviembre de 2016 a las 04:17 UTC
- Hora de edición: 26 de junio de 2020 a las 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAthenaFullAccess

AmazonAthenaFullAccess es una [política administrada de AWS](#) que proporciona acceso total a Amazon Athena y acceso limitado a las dependencias necesarias para permitir la consulta, la redacción de los resultados y la gestión de los datos.

Uso de esta política

Puede asociar AmazonAthenaFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 30 de noviembre de 2016 a las 16:46 UTC
- Hora editada: 3 de enero de 2024, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAugmentedAIFullAccess

AmazonAugmentedAIFullAccess es una [política administrada por AWS](#) que: proporciona acceso para realizar todas las operaciones con los recursos de IA aumentada de Amazon, incluidos FlowDefinitions, HumanTaskUis y HumanLoops. No permite el acceso para crear FlowDefinitions contra un equipo de trabajo público.

Uso de esta política

Puede asociar AmazonAugmentedAIFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 16:21 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAugmentedAIHumanLoopFullAccess

AmazonAugmentedAIHumanLoopFullAccess es una [política administrada por AWS](#) que: proporciona acceso para realizar todas las operaciones en HumanLoops.

Uso de esta política

Puede asociar AmazonAugmentedAIHumanLoopFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 16:20 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonAugmentedAIIntegratedAPIAccess

AmazonAugmentedAIIntegratedAPIAccess es una [política administrada por AWS](#) que: proporciona acceso para realizar todas las operaciones con los recursos de IA aumentada de Amazon, incluidos FlowDefinitions, HumanTaskUis y HumanLoops. También proporciona acceso a las operaciones de los servicios que están integrados con Amazon Augmented AI.

Uso de esta política

Puede asociar AmazonAugmentedAIIntegratedAPIAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de abril de 2020 a las 20:47 UTC

- Hora de edición: 22 de abril de 2020 a las 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonBedrockFullAccess

AmazonBedrockFullAccesses una [política AWS gestionada](#) que: proporciona acceso completo a Amazon Bedrock, así como acceso limitado a los servicios relacionados que necesite

Uso de la política

Puede asociar `AmazonBedrockFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de diciembre de 2023 a las 15:47 UTC
- Hora editada: 6 de diciembre de 2023 a las 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonBedrockReadOnly

AmazonBedrockReadOnly es una [política AWS gestionada](#) que: proporciona acceso de solo lectura a Amazon Bedrock

Uso de la política

Puede asociar AmazonBedrockReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de diciembre de 2023 a las 15:48 UTC
- Hora editada: 6 de diciembre de 2023 a las 15:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonBraketFullAccess

AmazonBraketFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Braket mediante AWS Management Console y SDK. También proporciona acceso a servicios relacionados (por ejemplo, S3 o registros).

Uso de esta política

Puede asociar AmazonBraketFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de agosto de 2020 a las 20:12 UTC
- Hora de edición: 19 de abril de 2023 a las 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonBraketJobsExecutionPolicy

AmazonBraketJobsExecutionPolicy es una [política administrada por AWS](#) que: otorga el acceso a Servicios de AWS y los recursos necesarios para ejecutar una tarea Amazon Braket, incluidos S3, Cloudwatch, IAM y Braket

Uso de esta política

Puede asociar AmazonBraketJobsExecutionPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de noviembre de 2021 a las 19:34 UTC
- Hora de edición: 28 de noviembre de 2021 a las 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Action" : [
      "braket:CancelJob",
      "braket:CancelQuantumTask",
      "braket:CreateJob",
      "braket:CreateQuantumTask",
      "braket:GetDevice",
      "braket:GetJob",
      "braket:GetQuantumTask",
      "braket:SearchDevices",
      "braket:SearchJobs",
      "braket:SearchQuantumTasks",
      "braket:ListTagsForResource",
      "braket:TagResource",
      "braket:UntagResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "braket.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles"
    ],
    "Resource" : "arn:aws:iam::*:role/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:GetQueryResults"
    ],
    "Resource" : [

```



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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonBraketServiceRolePolicy

AmazonBraketServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon Braket crear y gestionar recursos AWS en su nombre

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de agosto de 2020 a las 17:12 UTC
- Hora de edición: 6 de agosto de 2020 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    ],
    "Resource" : "arn:aws:s3:::amazon-braket-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:CreateLogGroup",
      "logs:DescribeLogGroups"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket:*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeFullAccess

AmazonChimeFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a la consola de administración de Amazon Chime a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonChimeFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de noviembre de 2017 a las 22:15 UTC
- Hora de edición: 14 de diciembre de 2020 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ]
    }
  ]
}
```

```
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:GetTopicAttributes"
    ],
    "Resource" : [
      "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:GetQueueAttributes",
      "sqs:CreateQueue"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
    ]
  },
  {
    "Action" : [
      "kinesis:ListStreams"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:DescribeStream"
    ],
    "Resource" : [
      "arn:aws:kinesis:*:*:stream/chime-chat-*",
      "arn:aws:kinesis:*:*:stream/chime-messaging-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
```

```
    "s3:GetEncryptionConfiguration",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::chime-chat-*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeReadOnly

AmazonChimeReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a la consola de administración de Amazon Chime a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonChimeReadOnly a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de noviembre de 2017 a las 22:04 UTC
- Hora de edición: 14 de diciembre de 2020 a las 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeSDK

AmazonChimeSDK es una [política administrada por AWS](#) que: proporciona acceso a las operaciones del Amazon Chime SDK

Uso de esta política

Puede asociar AmazonChimeSDK a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de febrero de 2020 a las 21:53 UTC
- Hora de edición: 10 de enero de 2023 a las 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMeeting",
        "chime:CreateMeetingWithAttendees",
        "chime>DeleteMeeting",
        "chime:GetMeeting",
        "chime:ListMeetings",
        "chime:CreateAttendee",
        "chime:BatchCreateAttendee",
        "chime>DeleteAttendee",
        "chime:GetAttendee",
        "chime:ListAttendees",
        "chime:ListAttendeeTags",
        "chime:ListMeetingTags",
```



```
    "chime:ListTagsForResource",
    "chime:TagAttendee",
    "chime:TagMeeting",
    "chime:TagResource",
    "chime:UntagAttendee",
    "chime:UntagMeeting",
    "chime:UntagResource",
    "chime:StartMeetingTranscription",
    "chime:StopMeetingTranscription",
    "chime:CreateMediaCapturePipeline",
    "chime:CreateMediaConcatenationPipeline",
    "chime:CreateMediaLiveConnectorPipeline",
    "chime>DeleteMediaCapturePipeline",
    "chime>DeleteMediaPipeline",
    "chime:GetMediaCapturePipeline",
    "chime:GetMediaPipeline",
    "chime:ListMediaCapturePipelines",
    "chime:ListMediaPipelines"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy es una [política AWS gestionada](#) que: Managed Policy for Amazon Chime SDK MediaPipelines Service Linked Role

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de abril de 2022 a las 22:02 UTC
- Hora editada: 8 de diciembre de 2023 a las 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Sid" : "AllowKinesisVideoStreamsAccess",
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:GetDataEndpoint",
      "kinesisvideo:PutMedia",
      "kinesisvideo:UpdateDataRetention",
      "kinesisvideo:DescribeStream",
      "kinesisvideo:CreateStream"
    ],
    "Resource" : [
      "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
    ]
  },
  {
    "Sid" : "AllowKinesisVideoStreamsListAccess",
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:ListStreams"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AllowChimeMeetingAccess",
    "Effect" : "Allow",
    "Action" : [
      "chime:GetMeeting",
      "chime:CreateAttendee",
      "chime>DeleteAttendee"
    ],
    "Resource" : "*"
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeSDKMessagingServiceRolePolicy

AmazonChimeSDKMessagingServiceRolePolicy es una [política administrada por AWS](#) que: permite que la mensajería del Amazon Chime SDK acceda a los recursos AWS y habilite la funcionalidad de mensajería

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de marzo de 2023 a la 01:43 UTC
- Hora de edición: 3 de marzo de 2023 a la 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeServiceRolePolicy

AmazonChimeServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los recursos AWS utilizados o administrados por Amazon Chime

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 30 de septiembre de 2019 a las 22:25 UTC
- Hora de edición: 30 de septiembre de 2019 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

AmazonChimeTranscriptionServiceLinkedRolePolicy es una [política administrada por AWS](#) que: permite a Amazon Chime acceder a Amazon Transcribe y Amazon Transcribe Medical en su nombre

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de agosto de 2021 a las 21:47 UTC
- Hora de edición: 4 de agosto de 2021 a las 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeUserManagement

AmazonChimeUserManagement es una [política administrada por AWS](#) que: proporciona acceso de administración de usuarios a la consola de administración de Amazon Chime a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonChimeUserManagement a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de noviembre de 2017 a las 22:17 UTC
- Hora de edición: 18 de febrero de 2020 a las 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroup",
        "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" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

AmazonChimeVoiceConnectorServiceLinkedRolePolicy es una [política administrada por AWS](#) que: sirve para el rol vinculado al servicio para Amazon Chime VoiceConnector

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de septiembre de 2019 a las 22:16 UTC
- Hora de edición: 14 de abril de 2023 a las 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMediaInsightsPipeline",
        "chime:GetMediaInsightsPipelineConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCloudDirectoryFullAccess

AmazonCloudDirectoryFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Cloud Directory Service.

Uso de esta política

Puede asociar AmazonCloudDirectoryFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de febrero de 2017 a las 00:41 UTC
- Hora de edición: 25 de febrero de 2017 a las 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCloudDirectoryReadOnlyAccess

AmazonCloudDirectoryReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a Amazon Cloud Directory Service.

Uso de esta política

Puede asociar AmazonCloudDirectoryReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de febrero de 2017 a las 23:42 UTC
- Hora de edición: 28 de febrero de 2017 a las 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCloudWatchEvidentlyFullAccess

AmazonCloudWatchEvidentlyFullAccess es una [política administrada por AWS](#) que proporciona acceso total y exclusivo a Amazon CloudWatch Evidently. También proporciona acceso a Amazon S3, Amazon SNS, Amazon CloudWatch y otros servicios relacionados.

Uso de esta política

Puede asociar `AmazonCloudWatchEvidentlyFullAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2021 a las 15:10 UTC
- Hora de edición: 29 de noviembre de 2021 a las 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Action" : [
  "iam:GetRole"
],
"Resource" : [
  "arn:aws:iam::*:role/service-role/CloudWatchRUMevidentlyRole-*"
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:DescribeAlarmHistory",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms",
    "cloudwatch:TagResource",
    "cloudwatch:UntagResource"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:LookupEvents"
  ],
  "Resource" : "*"
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:Evidently-Alarm-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:Subscribe",
    "sns:ListSubscriptionsByTopic"
  ],
  "Resource" : [
    "arn:*:sns:*:*:Evidently-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

AmazonCloudWatchEvidentlyReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon CloudWatch Evidently

Uso de esta política

Puede asociar AmazonCloudWatchEvidentlyReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2021 a las 15:08 UTC
- Hora de edición: 29 de noviembre de 2021 a las 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

AmazonCloudWatchEvidentlyServiceRolePolicy es una [política administrada por AWS](#) que: permite a CloudWatch Evidently Service administrar recursos asociados AWS en nombre del cliente

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de septiembre de 2022 a las 17:25 UTC
- Hora de edición: 13 de septiembre de 2022 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StartDeployment",
      "Resource" : [
        "arn:aws:appconfig:*:*:application/*",
        "arn:aws:appconfig:*:*:deploymentstrategy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StartDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/configurationprofile/*",
      "Condition" : {
        "StringNotEquals" : {
```

```

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

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCloudWatchRUMFullAccess

AmazonCloudWatchRUMFullAccess es una [política administrada por AWS](#) que: concede permisos de acceso total al servicio Amazon CloudWatch RUM

Uso de esta política

Puede asociar AmazonCloudWatchRUMFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2021 a las 15:46 UTC
- Hora de edición: 29 de noviembre de 2021 a las 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/rum.amazonaws.com/
AWSServiceRoleForRealUserMonitoring"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/RUM-Monitor*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "cognito-identity.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms"
  ],
  "Resource" : "arn:aws:cloudwatch::*:alarm:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cognito-identity:CreateIdentityPool",
    "cognito-identity:ListIdentityPools",
```



```

    "cognito-identity:DescribeIdentityPool",
    "cognito-identity:GetIdentityPoolRoles",
    "cognito-identity:SetIdentityPoolRoles"
  ],
  "Resource" : "arn:aws:cognito-identity:*:*:identitypool/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs>DeleteLogGroup",
    "logs:PutRetentionPolicy",
    "logs:CreateLogStream"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:*RUMService*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs>DeleteLogDelivery",
    "logs:ListLogDeliveries",
    "logs:DescribeResourcePolicies"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "synthetics:describeCanaries",
    "synthetics:describeCanariesLastRun"
  ],
  "Resource" : "arn:aws:synthetics:*:*:canary:*"
}
]

```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCloudWatchRUMReadOnlyAccess

AmazonCloudWatchRUMReadOnlyAccess es una [política administrada por AWS](#) que: concede permisos de solo lectura para el servicio Amazon CloudWatch RUM

Uso de esta política

Puede asociar AmazonCloudWatchRUMReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2021 a las 15:43 UTC
- Hora de edición: 28 de octubre de 2022 a las 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCloudWatchRUMServiceRolePolicy

AmazonCloudWatchRUMServiceRolePolicy es una [política administrada por AWS](#) que: le concede permiso al servicio Amazon CloudWatch RUM para publicar datos de monitoreo en otros servicios relevantes de AWS.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2021 a las 23:17 UTC
- Hora de edición: 22 de febrero de 2023 a las 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "RUM/CustomMetrics/*",
            "AWS/RUM"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeCatalystFullAccess

AmazonCodeCatalystFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a Amazon CodeCatalyst

Uso de esta política

Puede asociar AmazonCodeCatalystFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de abril de 2023 a las 16:50 UTC
- Hora de edición: 20 de abril de 2023 a las 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeCatalystReadOnlyAccess

AmazonCodeCatalystReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon CodeCatalyst

Uso de esta política

Puede asociar AmazonCodeCatalystReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de abril de 2023 a las 16:49 UTC
- Hora de edición: 20 de abril de 2023 a las 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeCatalystSupportAccess

AmazonCodeCatalystSupportAccess es una [política administrada por AWS](#) que: permite a Amazon CodeCatalyst crear, actualizar y resolver casos de AWS Support en su nombre.

Uso de esta política

Puede asociar AmazonCodeCatalystSupportAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 12:34 UTC
- Hora de edición: 20 de abril de 2023 a las 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeGuruProfilerAgentAccess

AmazonCodeGuruProfilerAgentAccess es una [política administrada por AWS](#) que: proporciona el acceso requerido por el agente Generador de perfiles de Amazon CodeGuru.

Uso de esta política

Puede asociar `AmazonCodeGuruProfilerAgentAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de febrero de 2021 a las 22:11 UTC
- Hora de edición: 5 de mayo de 2022 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeGuruProfilerFullAccess

AmazonCodeGuruProfilerFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo al Generador de perfiles de Amazon CodeGuru.

Uso de esta política

Puede asociar AmazonCodeGuruProfilerFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 10:13 UTC
- Hora de edición: 15 de julio de 2020 a las 3:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeGuruProfilerReadOnlyAccess

AmazonCodeGuruProfilerReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al Generador de perfiles de Amazon CodeGuru.

Uso de esta política

Puede asociar `AmazonCodeGuruProfilerReadOnlyAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 10:30 UTC
- Hora de edición: 27 de junio de 2020 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru:Get*",
        "codeguru-profiler:BatchGet*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeGuruReviewerFullAccess

AmazonCodeGuruReviewerFullAccess es una [política administrada por AWS](#) que: otorga acceso total al Revisor de Amazon CodeGuru y acceso limitado a las dependencias requeridas.

Uso de esta política

Puede asociar AmazonCodeGuruReviewerFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 8:33 UTC
- Hora de edición: 29 de agosto de 2020 a las 4:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

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

```

```

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

```



```
"Sid" : "CloudWatchEventsManagedRules",
"Effect" : "Allow",
"Action" : [
  "events:PutRule",
  "events:PutTargets",
  "events>DeleteRule",
  "events:RemoveTargets"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeGuruReviewerReadOnlyAccess

AmazonCodeGuruReviewerReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura al Revisor de Amazon CodeGuru.

Uso de esta política

Puede asociar AmazonCodeGuruReviewerReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 3 de diciembre de 2019 a las 8:48 UTC
- Hora de edición: 29 de agosto de 2020 a las 4:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeGuruReviewerServiceRolePolicy

AmazonCodeGuruReviewerServiceRolePolicy es una [política administrada por AWS](#) que: requiere un rol vinculado a un servicio para que el Revisor de Amazon CodeGuru pueda acceder a los recursos en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2019 a las 5:31 UTC
- Hora de edición: 27 de noviembre de 2020 a las 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCodeGuruReviewerEnabledRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetRepository",
        "codecommit:GetBranch",
        "codecommit:DescribePullRequestEvents",
```

```

    "codecommit:GetCommentsForPullRequest",
    "codecommit:GetDifferences",
    "codecommit:GetPullRequest",
    "codecommit:ListPullRequests",
    "codecommit:PostCommentForPullRequest",
    "codecommit:GitPull",
    "codecommit:UntagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/codeguru-reviewer" : "enabled"
    }
  }
},
{
  "Sid" : "AccessCodeGuruReviewerEnabledConnections",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "codestar-connections:ProviderAction" : [
        "ListBranches",
        "GetBranch",
        "ListRepositories",
        "ListOwners",
        "ListPullRequests",
        "GetPullRequest",
        "ListPullRequestComments",
        "ListPullRequestCommits",
        "ListCommitFiles",
        "ListBranchCommits",
        "CreatePullRequestDiffComment",
        "GitPull"
      ]
    }
  },
  "Null" : {
    "aws:ResourceTag/codeguru-reviewer" : "false"
  }
}
},

```

```
{
  "Sid" : "CloudWatchEventsResourceCleanup",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:RemoveTargets"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowGuruS3GetObject",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::codeguru-reviewer-*",
    "arn:aws:s3:::codeguru-reviewer-*/*"
  ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeGuruSecurityFullAccess

AmazonCodeGuruSecurityFullAccess es una [política administrada por AWS](#) que proporciona acceso total a Amazon CodeGuru Security.

Uso de esta política

Puede asociar `AmazonCodeGuruSecurityFullAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de mayo de 2023 a las 21:03 UTC
- Hora de edición: 9 de mayo de 2023 a las 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCodeGuruSecurityScanAccess

AmazonCodeGuruSecurityScanAccess es una [política administrada por AWS](#) que: proporciona el acceso necesario para trabajar con los escaneos de Amazon CodeGuru Security.

Uso de esta política

Puede asociar AmazonCodeGuruSecurityScanAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de mayo de 2023 a las 20:54 UTC
- Hora de edición: 09 de mayo de 2023 a las 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "codeguru-security:CreateScan",
    "codeguru-security:CreateUploadUrl",
    "codeguru-security:GetScan",
    "codeguru-security:GetFindings"
  ],
  "Resource" : "arn:aws:codeguru-security:*:*:scans/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCognitoDeveloperAuthenticatedIdentities

AmazonCognitoDeveloperAuthenticatedIdentities es una [política administrada por AWS](#) que: proporciona acceso a las API de Amazon Cognito para admitir las identidades autenticadas por los desarrolladores desde su servidor de autenticación.

Uso de esta política

Puede asociar AmazonCognitoDeveloperAuthenticatedIdentities a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de marzo de 2015 a las 17:22 UTC
- Hora de edición: 24 de marzo de 2015 a las 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCognitoIdpEmailServiceRolePolicy

AmazonCognitoIdpEmailServiceRolePolicy es una [política administrada por AWS](#) que permite que el servicio Amazon Cognito User Pools utilice sus identidades de SES para el envío de correos electrónicos

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de marzo de 2019 a las 21:32 UTC
- Hora de edición: 21 de marzo de 2019 a las 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "ses:List*"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCognitoIdpServiceRolePolicy

AmazonCognitoIdpServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y a los recursos usados o administrados por grupos de usuarios de Amazon Cognito

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de junio de 2020 a las 22:30 UTC
- Hora de edición: 26 de junio de 2020 a las 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCognitoPowerUser

AmazonCognitoPowerUser es una [política administrada por AWS](#) que: proporciona acceso administrativo a los recursos de Amazon Cognito existentes. Necesitará privilegios de administrador de Cuenta de AWS para crear nuevos recursos de Cognito.

Uso de esta política

Puede asociar AmazonCognitoPowerUser a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de marzo de 2015 a las 17:14 UTC
- Hora de edición: 1 de junio de 2021 a las 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    ],
    "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*"
    ]
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCognitoReadOnly

AmazonCognitoReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a los recursos de Amazon Cognito.

Uso de esta política

Puede asociar AmazonCognitoReadOnly a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de marzo de 2015 a las 17:06 UTC
- Hora de edición: 1 de agosto de 2019 a las 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:Describe*",
        "cognito-identity:Get*",
        "cognito-identity:List*",
        "cognito-idp:Describe*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:List*",
        "cognito-idp:Get*",

```

```
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "iam:ListOpenIdConnectProviders",
        "iam:ListRoles",
        "sns:ListPlatformApplications"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

AmazonCognitoUnAuthedIdentitiesSessionPolicy es una [política administrada por AWS](#) que: define el conjunto de permisos permitidos para las identidades no autenticadas para los grupos de identidades de Cognito. Esta política no está destinada a utilizarse como una política de permisos independiente. Se utiliza como barrera de protección contra las políticas excesivamente permisivas asociadas a las funciones de un grupo de identidades. No asocie esta política a ningún rol, ya que Cognito Identity Service la incluirá automáticamente como política restringida al crear credenciales. Los privilegios para acceder temporalmente a otros recursos de AWS a través del flujo mejorado se definirán ahora mediante la intersección del rol asociado a la identidad del usuario no autenticado proporcionado por un servicio y los privilegios otorgados en esta política administrada que es propiedad de Cognito.

Uso de esta política

Puede asociar AmazonCognitoUnAuthedIdentitiesSessionPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de julio de 2023 a las 23:04 UTC
- Hora de edición: 19 de julio de 2023 a las 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonCognitoUnauthenticatedIdentities

AmazonCognitoUnauthenticatedIdentities es una [política administrada por AWS](#) que: define el conjunto de permisos permitidos para las identidades no autenticadas para los grupos de identidades de Cognito. No es necesario que esté asociado a su rol de unauth, ya que Cognito Identity Service la incluirá automáticamente como una política restringida al crear las credenciales. Los privilegios para acceder temporalmente a otros recursos de AWS a través del flujo mejorado se definirán ahora mediante la intersección del rol asociado a la identidad del usuario no autenticado proporcionado por un servicio y los privilegios otorgados en esta política administrada que es propiedad de Cognito.

Uso de esta política

Puede asociar AmazonCognitoUnauthenticatedIdentities a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de febrero de 2023 a las 22:36 UTC
- Hora de edición: 1 de febrero de 2023 a las 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonConnect_FullAccess

AmazonConnect_FullAccess es una [política administrada por AWS](#) que: otorga a los usuarios de Connect AWS los permisos necesarios para usar los recursos de Connect. Esta política proporciona acceso total a los recursos de Connect AWS mediante la consola de Connect y las API públicas.

Uso de esta política

Puede asociar AmazonConnect_FullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de noviembre de 2020 a las 19:54 UTC
- Hora de edición: 7 de marzo de 2023 a las 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:*",
        "ds:CreateAlias",
        "ds:AuthorizeApplication",
        "ds:CreateIdentityPoolDirectory",
        "ds>DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:UnauthorizeApplication",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lex:GetBots",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:CreateLogGroup",
```

```

    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "lambda:ListFunctions",
    "ds:CheckAlias",
    "profile:ListAccountIntegrations",
    "profile:GetDomain",
    "profile:ListDomains",
    "profile:GetProfileObjectType",
    "profile:ListProfileObjectTypeTemplates"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "profile:AddProfileKey",
    "profile:CreateDomain",
    "profile:CreateProfile",
    "profile>DeleteDomain",
    "profile>DeleteIntegration",
    "profile>DeleteProfile",
    "profile>DeleteProfileKey",
    "profile>DeleteProfileObject",
    "profile>DeleteProfileObjectType",
    "profile:GetIntegration",
    "profile:GetMatches",
    "profile:GetProfileObjectType",
    "profile:ListIntegrations",
    "profile:ListProfileObjects",
    "profile:ListProfileObjectTypes",
    "profile:ListTagsForResource",
    "profile:MergeProfiles",
    "profile:PutIntegration",
    "profile:PutProfileObject",
    "profile:PutProfileObjectType",
    "profile:SearchProfiles",
    "profile:TagResource",
    "profile:UntagResource",
    "profile:UpdateDomain",
    "profile:UpdateProfile"
  ],
  "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:GetBucketAcl"
    ],
    "Resource" : "arn:aws:s3:::amazon-connect-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:GetServiceQuota"
    ],
    "Resource" : "arn:aws:servicequotas:*:*:connect/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "connect.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:DeleteServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "profile.amazonaws.com"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

AmazonConnectCampaignsServiceLinkedRolePolicy es una [política administrada de AWS](#) que tiene roles vinculados al servicio de campañas de Amazon Connect

Uso de esta política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de septiembre de 2021 a las 20:54 UTC
- Hora de edición: 8 de noviembre de 2023 a las 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonConnectReadOnlyAccess

AmazonConnectReadOnlyAccess es una [política administrada por AWS](#) que: otorga permiso para ver las instancias de Amazon Connect en su Cuenta de AWS.

Uso de esta política

Puede asociar AmazonConnectReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de octubre de 2018 a las 21:00 UTC
- Hora de edición: 6 de noviembre de 2019 a las 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonConnectServiceLinkedRolePolicy

AmazonConnectServiceLinkedRolePolicy es una [política administrada de AWS](#) que permite a Amazon Connect crear y gestionar recursos de AWS en su nombre.

Uso de esta política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de septiembre de 2018 a las 00:21 UTC
- Hora editada: 28 de noviembre de 2023, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid" : "AllowS3ObjectForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*/*"
      ]
    },
    {
      "Sid" : "AllowGetBucketMetadataForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",

```

```
    "s3:GetBucketAcl"
  ],
  "Resource" : [
    "arn:aws:s3:::amazon-connect-*"
  ]
},
{
  "Sid" : "AllowConnectLogGroupAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
  ]
},
{
  "Sid" : "AllowListLexBotAccess",
  "Effect" : "Allow",
  "Action" : [
    "lex:ListBots",
    "lex:ListBotAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowCustomerProfilesForConnectDomain",
  "Effect" : "Allow",
  "Action" : [
    "profile:SearchProfiles",
    "profile:CreateProfile",
    "profile:UpdateProfile",
    "profile:AddProfileKey",
    "profile:ListProfileObjectTypes",
    "profile:ListCalculatedAttributeDefinitions",
    "profile:ListCalculatedAttributesForProfile",
    "profile:GetDomain",
    "profile:ListIntegrations"
  ],
  "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}"
      }
    }
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonConnectSynchronizationServiceRolePolicy

AmazonConnectSynchronizationServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon Connect sincronizar recursos de AWS entre regiones en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de octubre de 2023 a las 22:38 UTC
- Hora de edición: 27 de octubre de 2023 a las 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
    }
  }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonConnectVoiceIDFullAccess

AmazonConnectVoiceIDFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Connect Voice ID

Uso de esta política

Puede asociar AmazonConnectVoiceIDFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 26 de septiembre de 2021 a las 19:04 UTC
- Hora de edición: 26 de septiembre de 2021 a las 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDataZoneDomainExecutionRolePolicy

AmazonDataZoneDomainExecutionRolePolicy es una [política AWS gestionada](#) que: Política predeterminada para el rol DataZone de DomainExecutionRole servicio de Amazon. Amazon utiliza esta función DataZone para catalogar, descubrir, gobernar, compartir y analizar datos en el DataZone dominio de Amazon.

Uso de la política

Puede asociar AmazonDataZoneDomainExecutionRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de septiembre de 2023 a las 21:55 UTC
- Hora editada: 12 de marzo de 2024 a las 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

AmazonDataZoneEnvironmentRolePermissionsBoundary es una [política AWS gestionada](#) que: Amazon DataZone crea funciones de IAM para que los entornos realicen acciones de análisis de datos y utiliza esta política al crear estas funciones para definir el límite de sus permisos.

Uso de la política

Puede asociar AmazonDataZoneEnvironmentRolePermissionsBoundary a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 11 de septiembre de 2023 a las 23:38 UTC
- Hora editada: 17 de noviembre de 2023 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Sid" : "GlueOperations",
"Effect" : "Allow",
"Action" : [
  "glue:*DataQuality*",
  "glue:BatchCreatePartition",
  "glue:BatchDeleteConnection",
  "glue:BatchDeletePartition",
  "glue:BatchDeleteTable",
  "glue:BatchDeleteTableVersion",
  "glue:BatchGetJobs",
  "glue:BatchGetWorkflows",
  "glue:BatchStopJobRun",
  "glue:BatchUpdatePartition",
  "glue:CreateBlueprint",
  "glue:CreateConnection",
  "glue:CreateCrawler",
  "glue:CreateDatabase",
  "glue:CreateJob",
  "glue:CreatePartition",
  "glue:CreatePartitionIndex",
  "glue:CreateTable",
  "glue:CreateWorkflow",
  "glue>DeleteBlueprint",
  "glue>DeleteColumnStatisticsForPartition",
  "glue>DeleteColumnStatisticsForTable",
  "glue>DeleteConnection",
  "glue>DeleteCrawler",
  "glue>DeleteJob",
  "glue>DeletePartition",
  "glue>DeletePartitionIndex",
  "glue>DeleteTable",
  "glue>DeleteTableVersion",
  "glue>DeleteWorkflow",
  "glue:GetColumnStatisticsForPartition",
  "glue:GetColumnStatisticsForTable",
  "glue:GetConnection",
  "glue:GetDatabase",
  "glue:GetDatabases",
  "glue:GetTable",
  "glue:GetTables",
  "glue:GetPartition",
  "glue:GetPartitions",
  "glue:ListSchemas",
  "glue:ListJobs",
```

```

    "glue:NotifyEvent",
    "glue:PutWorkflowRunProperties",
    "glue:ResetJobBookmark",
    "glue:ResumeWorkflowRun",
    "glue:SearchTables",
    "glue:StartBlueprintRun",
    "glue:StartCrawler",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:StartWorkflowRun",
    "glue:StopCrawler",
    "glue:StopCrawlerSchedule",
    "glue:StopWorkflowRun",
    "glue:UpdateBlueprint",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:UpdateConnection",
    "glue:UpdateCrawler",
    "glue:UpdateCrawlerSchedule",
    "glue:UpdateDatabase",
    "glue:UpdateJob",
    "glue:UpdatePartition",
    "glue:UpdateTable",
    "glue:UpdateWorkflow"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "PassRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/datazone*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "glue.amazonaws.com"
    }
  }
}

```

```

    }
  }
},
{
  "Sid" : "SameAccountKmsOperations",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "KmsOperationsWithResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:Verify",
    "kms:Sign"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "AnalyticsOperations",
  "Effect" : "Allow",
  "Action" : [
    "datazone:*",
    "sqlworkbench:*"
  ],

```

```
"Resource" : "*"
},
{
  "Sid" : "QueryOperations",
  "Effect" : "Allow",
  "Action" : [
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena>DeleteNamedQuery",
    "athena>DeleteNotebook",
    "athena>DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
```

```
"athena:UpdateNotebookMetadata",
"athena:UpdatePreparedStatement",
"ec2:CreateNetworkInterface",
"ec2:DeleteNetworkInterface",
"ec2:Describe*",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition",
"glue:BatchDeleteTable",
"glue:BatchDeleteTableVersion",
"glue:BatchGetJobs",
"glue:BatchGetPartition",
"glue:BatchGetWorkflows",
"glue:BatchUpdatePartition",
"glue:CreateBlueprint",
"glue:CreateConnection",
"glue:CreateCrawler",
"glue:CreateDatabase",
"glue:CreateJob",
"glue:CreatePartition",
"glue:CreatePartitionIndex",
"glue:CreateTable",
"glue:CreateWorkflow",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeletePartition",
"glue>DeletePartitionIndex",
"glue>DeleteTable",
"glue>DeleteTableVersion",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:GetConnection",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetTable",
"glue:GetTables",
"glue:GetPartition",
"glue:GetPartitions",
"glue:ListSchemas",
"glue:ListJobs",
"glue:NotifyEvent",
"glue:SearchTables",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:UpdateDatabase",
```

```
"glue:UpdatePartition",
"glue:UpdateTable",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:ListGroups",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListUsers",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:DescribeMetricFilters",
"logs:DescribeQueries",
"logs:DescribeQueryDefinitions",
"logs:DescribeMetricFilters",
"logs:StartQuery",
"logs:StopQuery",
"logs:GetLogEvents",
"logs:GetLogGroupFields",
"logs:GetQueryResults",
"logs:GetLogRecord",
"logs:PutLogEvents",
"logs:CreateLogStream",
"logs:FilterLogEvents",
"lakeformation:GetDataAccess",
"lakeformation:GetDataLakeSettings",
"lakeformation:GetResourceLFTags",
"lakeformation:ListPermissions",
"redshift-data:ListTables",
"redshift-data:DescribeTable",
"redshift-data:ListSchemas",
"redshift-data:ListDatabases",
"redshift-data:ExecuteStatement",
"redshift-data:GetStatementResult",
"redshift-data:DescribeStatement",
"redshift:CreateClusterUser",
"redshift:DescribeClusters",
"redshift:DescribeDataShares",
"redshift:GetClusterCredentials",
"redshift:GetClusterCredentialsWithIAM",
"redshift:JoinGroup",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListWorkgroups",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetWorkgroup",
```

```

    "redshift-serverless:GetCredentials",
    "secretsmanager:ListSecrets",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "QueryOperationsWithResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "athena:GetQueryResultsStream"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "SecretsManagerOperationsWithTagKeys",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AmazonDataZoneDomain" : "*",
      "aws:ResourceTag/AmazonDataZoneProject" : "*"
    },
    "Null" : {
      "aws:TagKeys" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AmazonDataZoneDomain",
        "AmazonDataZoneProject"
      ]
    }
  }
},
{

```

```

    "Sid" : "DataZoneS3Buckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:GetObject",
      "s3:PutObject",
      "s3:PutObjectRetention",
      "s3:ReplicateObject",
      "s3:RestoreObject"
    ],
    "Resource" : [
      "arn:aws:s3::*/datazone/*"
    ]
  },
  {
    "Sid" : "DataZoneS3BucketLocation",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ListDataZoneS3Bucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "s3:prefix" : [
          "*/datazone/*",
          "datazone/*"
        ]
      }
    }
  }
},
{
  "Sid" : "NotDeniedOperations",

```



```
"Effect" : "Deny",
"NotAction" : [
  "datazone:*",
  "sqlworkbench:*",
  "athena:BatchGetNamedQuery",
  "athena:BatchGetPreparedStatement",
  "athena:BatchGetQueryExecution",
  "athena:CreateNamedQuery",
  "athena:CreateNotebook",
  "athena:CreatePreparedStatement",
  "athena:CreatePresignedNotebookUrl",
  "athena>DeleteNamedQuery",
  "athena>DeleteNotebook",
  "athena>DeletePreparedStatement",
  "athena:ExportNotebook",
  "athena:GetDatabase",
  "athena:GetDataCatalog",
  "athena:GetNamedQuery",
  "athena:GetPreparedStatement",
  "athena:GetQueryExecution",
  "athena:GetQueryResults",
  "athena:GetQueryResultsStream",
  "athena:GetQueryRuntimeStatistics",
  "athena:GetTableMetadata",
  "athena:GetWorkGroup",
  "athena:ImportNotebook",
  "athena:ListDatabases",
  "athena:ListDataCatalogs",
  "athena:ListEngineVersions",
  "athena:ListNamedQueries",
  "athena:ListPreparedStatements",
  "athena:ListQueryExecutions",
  "athena:ListTableMetadata",
  "athena:ListTagsForResource",
  "athena:ListWorkGroups",
  "athena:StartCalculationExecution",
  "athena:StartQueryExecution",
  "athena:StartSession",
  "athena:StopCalculationExecution",
  "athena:StopQueryExecution",
  "athena:TerminateSession",
  "athena:UpdateNamedQuery",
  "athena:UpdateNotebook",
  "athena:UpdateNotebookMetadata",
```

```
"athena:UpdatePreparedStatement",
"ec2:CreateNetworkInterface",
"ec2:CreateTags",
"ec2>DeleteNetworkInterface",
"ec2>DeleteTags",
"ec2:Describe*",
"glue:*DataQuality*",
"glue:BatchCreatePartition",
"glue:BatchDeleteConnection",
"glue:BatchDeletePartition",
"glue:BatchDeleteTable",
"glue:BatchDeleteTableVersion",
"glue:BatchGetJobs",
"glue:BatchGetPartition",
"glue:BatchGetWorkflows",
"glue:BatchStopJobRun",
"glue:BatchUpdatePartition",
"glue:CreateBlueprint",
"glue:CreateConnection",
"glue:CreateCrawler",
"glue:CreateDatabase",
"glue:CreateJob",
"glue:CreatePartition",
"glue:CreatePartitionIndex",
"glue:CreateTable",
"glue:CreateWorkflow",
"glue>DeleteBlueprint",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeleteConnection",
"glue>DeleteCrawler",
"glue>DeleteJob",
"glue>DeletePartition",
"glue>DeletePartitionIndex",
"glue>DeleteTable",
"glue>DeleteTableVersion",
"glue>DeleteWorkflow",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:GetConnection",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetTable",
"glue:GetTables",
```

```
"glue:GetPartition",
"glue:GetPartitions",
"glue:ListSchemas",
"glue:ListJobs",
"glue:NotifyEvent",
"glue:PutWorkflowRunProperties",
"glue:ResetJobBookmark",
"glue:ResumeWorkflowRun",
"glue:SearchTables",
"glue:StartBlueprintRun",
"glue:StartCrawler",
"glue:StartCrawlerSchedule",
"glue:StartJobRun",
"glue:StartWorkflowRun",
"glue:StopCrawler",
"glue:StopCrawlerSchedule",
"glue:StopWorkflowRun",
"glue:UpdateBlueprint",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:UpdateConnection",
"glue:UpdateCrawler",
"glue:UpdateCrawlerSchedule",
"glue:UpdateDatabase",
"glue:UpdateJob",
"glue:UpdatePartition",
"glue:UpdateTable",
"glue:UpdateWorkflow",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:List*",
"iam:PassRole",
"kms:DescribeKey",
"kms:Decrypt",
"kms:Encrypt",
"kms:GenerateDataKey",
"kms:ListKeys",
"kms:Verify",
"kms:Sign",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:DescribeMetricFilters",
"logs:DescribeQueries",
"logs:DescribeQueryDefinitions",
```

```
"logs:StartQuery",
"logs:StopQuery",
"logs:GetLogEvents",
"logs:GetLogGroupFields",
"logs:GetQueryResults",
"logs:GetLogRecord",
"logs:PutLogEvents",
"logs:CreateLogStream",
"logs:FilterLogEvents",
"lakeformation:GetDataAccess",
"lakeformation:GetDataLakeSettings",
"lakeformation:GetResourceLFTags",
"lakeformation:ListPermissions",
"redshift-data:ListTables",
"redshift-data:DescribeTable",
"redshift-data:ListSchemas",
"redshift-data:ListDatabases",
"redshift-data:ExecuteStatement",
"redshift-data:GetStatementResult",
"redshift-data:DescribeStatement",
"redshift:CreateClusterUser",
"redshift:DescribeClusters",
"redshift:DescribeDataShares",
"redshift:GetClusterCredentials",
"redshift:GetClusterCredentialsWithIAM",
"redshift:JoinGroup",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListWorkgroups",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:GetCredentials",
"s3:AbortMultipartUpload",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:GetObject",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:PutObject",
"s3:PutObjectRetention",
"s3:ReplicateObject",
"s3:RestoreObject",
"secretsmanager:CreateSecret",
"secretsmanager:ListSecrets",
"secretsmanager:TagResource",
```

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDataZoneFullAccess

AmazonDataZoneFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a Amazon DataZone a través de los servicios relacionados que requiera, así AWS Management Console como acceso limitado a ellos.

Uso de la política

Puede asociar AmazonDataZoneFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de septiembre de 2023 a las 20:06 UTC
- Hora editada: 12 de marzo de 2024 a las 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2: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_*"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonDataZoneFullUserAccess

AmazonDataZoneFullUserAccesses una [política AWS gestionada](#) que: proporciona acceso total a Amazon DataZone, pero no permite la gestión de dominios, usuarios o cuentas asociadas.

Uso de la política

Puede asociar AmazonDataZoneFullUserAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 22 de septiembre de 2023 a las 21:06 UTC
- Hora editada: 12 de marzo de 2024 a las 23:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```

}

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonDataZoneGlueManageAccessRolePolicy

AmazonDataZoneGlueManageAccessRolePolicy es una [política AWS gestionada](#) que:

La política concede permisos para permitir que Amazon habilite DataZone la publicación y las concesiones de acceso a los datos.

Uso de la política

Puede asociar AmazonDataZoneGlueManageAccessRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de septiembre de 2023 a las 20:21 UTC
- Hora editada: 14 de diciembre de 2023 a las 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDataZonePortalFullAccessPolicy

AmazonDataZonePortalFullAccessPolicy es una [política administrada por AWS](#) que proporciona acceso completo a las API de Amazon DataZone

Uso de esta política

Puede asociar AmazonDataZonePortalFullAccessPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de marzo de 2023 a las 18:24 UTC
- Hora de edición: 26 de marzo de 2023 a las 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDataZonePreviewConsoleFullAccess

AmazonDataZonePreviewConsoleFullAccess es una [política administrada por AWS](#) que proporciona acceso completo a la versión preliminar de Amazon DataZone a través de AWS Management Console. También proporciona acceso selecto a otros servicios relacionados.

Uso de esta política

Puede asociar AmazonDataZonePreviewConsoleFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de marzo de 2023 a las 15:16 UTC
- Hora de edición: 13 de julio de 2023 a las 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListAliases",
      "glue:GetConnections",
      "glue:GetDatabase",
      "redshift:DescribeClusters",
      "ec2:DescribeSubnets",
      "secretsmanager:ListSecrets",
      "iam:ListRoles",
      "sso:DescribeRegisteredRegions"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateConnection"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:connection/AmazonDataZone-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:GetPolicy",
    "Resource" : [
      "arn:aws:iam:*:*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-AmazonDataZoneBootstrapRole",
      "arn:aws:iam:*:*:policy/service-role/AmazonDataZoneServicePolicy-AmazonDataZoneServiceRole"
    ]
  },
  {

```

```
"Effect" : "Allow",
"Action" : "iam:PassRole",
"Resource" : [
  "arn:aws:iam::*:role/AmazonDataZoneServiceRole*",
  "arn:aws:iam::*:role/service-role/AmazonDataZoneServiceRole*",
  "arn:aws:iam::*:role/AmazonDataZoneBootstrapRole*",
  "arn:aws:iam::*:role/service-role/AmazonDataZoneBootstrapRole",
  "arn:aws:iam::*:role/AmazonDataZoneDomainExecutionRole",
  "arn:aws:iam::*:role/service-role/AmazonDataZoneDomainExecutionRole"
],
"Condition" : {
  "StringEquals" : {
    "iam:passedToService" : "datazonecontrol.amazonaws.com"
  }
}
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

AmazonDataZoneProjectDeploymentPermissionsBoundary es una [política administrada por AWS](#), Amazon DataZone, que crea roles de IAM que utiliza para implementar proyectos de análisis de datos. DataZone utiliza esta política al crear estos roles para definir el límite de sus permisos.

Uso de esta política

Puede asociar AmazonDataZoneProjectDeploymentPermissionsBoundary a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de marzo de 2023 a las 2:54 UTC
- Hora de edición: 4 de abril de 2023 a las 2:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam>DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "iam:DeleteRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/*datazone*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateKey",
      "kms:TagResource",
      "athena:CreateWorkGroup",
      "athena:TagResource",
      "iam:TagRole",
      "iam:TagPolicy",
      "logs:CreateLogGroup",
      "logs:TagLogGroup",
      "ssm:AddTagsToResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : "datazone:*"
      },
      "StringLike" : {
        "aws:ResourceTag/datazone:projectId" : "proj-*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "athena>DeleteWorkGroup",
      "kms:ScheduleKeyDeletion",
      "kms:DescribeKey",
      "kms:EnableKeyRotation",
      "kms:DisableKeyRotation",
      "kms:GenerateDataKey",
      "kms:Encrypt",
      "kms:Decrypt",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress"
    ],
  },

```

```
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "aws:ResourceTag/datazone:projectId" : "proj-*"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : "datazone:projectId"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:DeletePolicy",
    "s3:DeleteBucket"
  ],
  "Resource" : [
    "arn:aws:iam::*:policy/datazone*",
    "arn:aws:s3:::datazone*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter*",
    "ssm:PutParameter",
    "ssm>DeleteParameter"
  ],
  "Resource" : [
    "arn:aws:ssm::*:parameter/*datazone*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
```



```

    "iam:GetRole",
    "iam:GetPolicy",
    "iam:GetRolePolicy",
    "iam:CreatePolicy",
    "iam:ListPolicyVersions",
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
    "lakeformation:PutDataLakeSettings",
    "lakeformation:GetDataLakeSettings",
    "lakeformation:RevokePermissions",
    "lakeformation:ListPermissions",
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue:GetDatabases",
    "glue:GetDatabase",
    "sts:GetCallerIdentity"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/*datazone*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketPublicAccessBlock",
    "s3>DeleteBucketPolicy",
    "s3:CreateBucket",
    "s3:PutBucketPolicy",
    "s3:PutBucketAcl",
    "s3:PutBucketVersioning",
    "s3:PutBucketTagging",
    "s3:PutBucketLogging",
    "s3:GetObject*",
    "s3:GetBucket*",
    "s3:List*"
  ],

```

```

    "s3:GetEncryptionConfiguration",
    "s3:DeleteObject*",
    "s3:PutObject*",
    "s3:Abort*"
  ],
  "Resource" : "arn:aws:s3::*datazone*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "athena:Get*",
    "athena:List*",
    "ec2:CreateSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2>DeleteSecurityGroup",
    "ec2:Describe*",
    "ec2:Get*",
    "ec2:List*",
    "logs:PutRetentionPolicy",
    "logs:DescribeLogGroups",
    "logs>DeleteLogGroup",
    "logs>DeleteRetentionPolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:PutKeyPolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
},

```

```
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateVpcEndpoint",
  "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringLike" : {
      "ec2:VpceServiceName" : [
        "com.amazonaws.*.logs",
        "com.amazonaws.*.s3",
        "com.amazonaws.*.glue",
        "com.amazonaws.*.athena"
      ]
    }
  }
},
{
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:GetTemplate",
    "cloudformation:DescribeChangeSet",
    "cloudformation:CreateChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation>DeleteChangeSet",
    "cloudformation:CreateStack",
    "cloudformation:UpdateStack",
    "cloudformation>DeleteStack",
    "cloudformation:TagResource",
    "cloudformation:GetTemplateSummary"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/DataZone*"
  ]
},
{
  "Effect" : "Deny",
```

```

    "Action" : [
      "s3:GetObject*",
      "s3:GetBucket*",
      "s3:List*",
      "s3:GetEncryptionConfiguration",
      "s3:DeleteObject*",
      "s3:PutObject*",
      "s3:Abort*",
      "s3:DeleteBucket"
    ],
    "NotResource" : [
      "arn:aws:s3::*datazone*"
    ]
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "kms:*"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringNotEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Effect" : "Deny",
    "NotAction" : [
      "ssm:PutParameter",
      "ssm:DeleteParameter",
      "ssm:AddTagsToResource",
      "ssm:GetParameters",
      "ssm:GetParameter",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketPublicAccessBlock",
      "s3:DeleteBucketPolicy",
      "s3:CreateBucket",
      "s3:PutBucketAcl",
      "s3:PutBucketPolicy",
      "s3:PutBucketVersioning",
      "s3:PutBucketTagging",
      "s3:ListBucket",
      "s3:PutBucketLogging",

```

```
"s3:DeleteBucket",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetPolicy",
"iam:CreatePolicy",
"iam:ListPolicyVersions",
"iam:DeletePolicy",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:GetTemplate",
"cloudformation:DescribeChangeSet",
"cloudformation:CreateChangeSet",
"cloudformation:ExecuteChangeSet",
"cloudformation:DeleteChangeSet",
"cloudformation:TagResource",
"cloudformation:CreateStack",
"cloudformation:UpdateStack",
"cloudformation:DeleteStack",
"cloudformation:GetTemplateSummary",
"athena:*",
"kms:*",
"glue:CreateDatabase",
"glue>DeleteDatabase",
"glue:GetDatabases",
"glue:GetDatabase",
"lambda:*",
"ec2:*",
"logs:*",
"servicecatalog:CreateApplication",
"servicecatalog>DeleteApplication",
"servicecatalog:GetApplication",
"lakeformation:RegisterResource",
"lakeformation:DeregisterResource",
"lakeformation:GrantPermissions",
"lakeformation:PutDataLakeSettings",
"lakeformation:RevokePermissions",
"lakeformation:GetDataLakeSettings",
"lakeformation:ListPermissions",
"iam:CreateRole",
"iam>DeleteRole",
"iam:DetachRolePolicy",
"iam>DeleteRolePolicy",
"iam:AttachRolePolicy",
"iam:PutRolePolicy",
```

```
    "iam:UntagRole",
    "iam:PassRole",
    "iam:TagRole",
    "s3:GetBucket*",
    "s3:GetObject*",
    "s3:Abort*",
    "s3:GetEncryptionConfiguration",
    "s3:PutObject*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDataZoneProjectRolePermissionsBoundary

AmazonDataZoneProjectRolePermissionsBoundary es una [política administrada por AWS](#), Amazon DataZone, que crea roles de IAM para que los proyectos realicen acciones de análisis de datos y utiliza esta política al crear estas funciones para definir el límite de sus permisos.

Uso de esta política

Puede asociar AmazonDataZoneProjectRolePermissionsBoundary a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 21 de marzo de 2023 a las 2:51 UTC
- Hora de edición: 21 de marzo de 2023 a las 2:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "s3:List*",
      "s3:Get*",
      "kms:List*",
      "kms:Get*",
      "kms:Describe*",
      "kms:Decrypt"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringNotEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:Describe*",
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterface",
      "logs:*",
      "athena:TerminateSession",
      "athena:CreatePreparedStatement",
      "athena:StopCalculationExecution",
      "athena:StartQueryExecution",
      "athena:UpdatePreparedStatement",
      "athena:BatchGet*",
      "athena:List*",
      "athena:UpdateNotebook",
      "athena>DeleteNotebook",
      "athena>DeletePreparedStatement",
      "athena:UpdateNotebookMetadata",
      "athena>DeleteNamedQuery",
      "athena:Get*",
      "athena:UpdateNamedQuery",
      "athena:CreateNamedQuery",
      "athena:ExportNotebook",
      "athena:StopQueryExecution",
      "athena:StartCalculationExecution",
      "athena:StartSession",
      "athena:CreatePresignedNotebookUrl",
      "athena:CreateNotebook",
      "athena:ImportNotebook",

```



```
"organizations:DescribeOrganization",
"organizations:DescribeAccount",
"lakeformation:GetDataAccess",
"lakeformation:BatchGrantPermissions",
"lakeformation:GrantPermissions",
"lakeformation:GetDataLakeSettings",
"lakeformation:PutDataLakeSettings",
"lakeformation:BatchRevokePermissions",
"lakeformation:GetResourceLFTags",
"lakeformation:ListPermissions",
"ram:CreateResourceShare",
"ram:UpdateResourceShare",
"ram>DeleteResourceShare",
"ram:AssociateResourceShare",
"ram:DisassociateResourceShare",
"ram:AcceptResourceShareInvitation",
"ram:Get*",
"ram:List*",
"redshift:DescribeClusters",
"redshift:JoinGroup",
"redshift:CreateClusterUser",
"redshift:GetClusterCredentials",
"redshift-data:*",
"redshift:AuthorizeDataShare",
"redshift:DescribeDataShares",
"redshift:AssociateDataShareConsumer",
"tag:GetResources",
"iam:ListRoles",
"iam:ListUsers",
"iam:ListGroups",
"iam:ListRolePolicies",
"iam:GetRole",
"iam:GetRolePolicy",
"glue:CreateTable",
"glue:BatchCreatePartition",
"glue:CreatePartition",
"glue:CreatePartitionIndex",
"glue:CreateDataQualityRuleset",
"glue:CreateBlueprint",
"glue:CreateJob",
"glue:CreateConnection",
"glue:CreateCrawler",
"glue:CreateWorkflow",
"sqlworkbench:*",
```

```

    "datazone:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws-glue-service-resource"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:List*",
    "kms:Get*",
    "kms:Describe*",
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Verify",
    "kms:Sign",
    "kms:GenerateDataKey",
    "glue:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/datazone:projectId" : "false"
    }
  }
},
{
  "Effect" : "Allow",

```

```
"Action" : [
  "iam:PassRole"
],
"Resource" : [
  "arn:aws:iam::*:role/datazone*"
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:BatchGet*",
    "glue:SearchTables",
    "glue:List*",
    "glue:Get*",
    "glue:CreateDatabase",
    "glue:UpdateDatabase",
    "glue>DeleteTable",
    "glue:BatchDeleteTable",
    "glue:UpdateTable",
    "glue>DeletePartition",
    "glue:BatchDeletePartition",
    "glue:PutResourcePolicy",
    "glue:BatchUpdatePartition",
    "glue>DeleteTableVersion",
    "glue>DeleteColumnStatisticsForPartition",
    "glue>DeleteColumnStatisticsForTable",
    "glue>DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:UpdatePartition",
    "glue:NotifyEvent",
    "glue>DeleteResourcePolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Deny",
  "NotAction" : [
    "s3:List*",
    "s3:Get*",
    "s3:Describe*",
    "s3>DeleteObjectVersion",
    "s3:RestoreObject",
```

```
"s3:ReplicateObject",
"s3:PutObject",
"s3:AbortMultipartUpload",
"s3:CreateBucket",
"s3:PutBucketPublicAccessBlock",
"s3:PutObjectRetention",
"s3>DeleteObject",
"kms:List*",
"kms:Get*",
"kms:Describe*",
"kms:Decrypt",
"kms:Encrypt",
"kms:ReEncrypt*",
"kms:Verify",
"kms:Sign",
"kms:GenerateDataKey",
"ec2:Describe*",
"ec2:CreateNetworkInterface",
"ec2>DeleteNetworkInterface",
"ec2:CreateTags",
"ec2>DeleteTags",
"logs:*",
"athena:*",
"glue:BatchGet*",
"glue:Get*",
"glue:SearchTables",
"glue:List*",
"glue:CreateDatabase",
"glue:UpdateDatabase",
"glue:CreateTable",
"glue>DeleteTable",
"glue:BatchDeleteTable",
"glue:UpdateTable",
"glue:BatchCreatePartition",
"glue:CreatePartition",
"glue>DeletePartition",
"glue:BatchDeletePartition",
"glue:PutResourcePolicy",
"glue:CreatePartitionIndex",
"glue:BatchUpdatePartition",
"glue>DeleteTableVersion",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeletePartitionIndex",
```

```
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:BatchDeleteTableVersion",
"glue:UpdatePartition",
"glue:NotifyEvent",
"glue:StartBlueprintRun",
"glue:PutWorkflowRunProperties",
"glue:StopCrawler",
"glue:DeleteJob",
"glue:DeleteWorkflow",
"glue:UpdateCrawler",
"glue:DeleteBlueprint",
"glue:UpdateWorkflow",
"glue:StartCrawler",
"glue:ResetJobBookmark",
"glue:UpdateJob",
"glue:StartWorkflowRun",
"glue:StopCrawlerSchedule",
"glue:ResumeWorkflowRun",
"glue:DeleteCrawler",
"glue:UpdateBlueprint",
"glue:BatchStopJobRun",
"glue:StopWorkflowRun",
"glue:UpdateCrawlerSchedule",
"glue:DeleteConnection",
"glue:UpdateConnection",
"glue:BatchDeleteConnection",
"glue:StartCrawlerSchedule",
"glue:StartJobRun",
"glue:CreateWorkflow",
"glue:*DataQuality*",
"glue:CreateBlueprint",
"glue:CreateJob",
"glue:CreateConnection",
"glue:CreateCrawler",
"glue>DeleteResourcePolicy",
"organizations:DescribeOrganization",
"organizations:DescribeAccount",
"lakeformation:GetDataAccess",
"lakeformation:BatchGrantPermissions",
"lakeformation:GrantPermissions",
"lakeformation:GetDataLakeSettings",
"lakeformation:PutDataLakeSettings",
"lakeformation:BatchRevokePermissions",
```

```
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListPermissions",
    "iam:*",
    "redshift:*",
    "redshift-data:*",
    "tag:GetResources",
    "iam:List*",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:PassRole",
    "sqlworkbench:*",
    "datazone:*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

AmazonDataZoneRedshiftGlueProvisioningPolicy es una [política AWS gestionada](#) que: Amazon DataZone es un servicio de gestión de datos que le permite catalogar, descubrir, gobernar, compartir y analizar sus datos. Con Amazon DataZone, puedes compartir tus datos y acceder a ellos en todas las cuentas y regiones compatibles. Amazon DataZone simplifica su experiencia en todos AWS los servicios, incluidos, entre otros, Amazon Redshift, Amazon Athena, AWS Glue y Lake Formation. AWS

Uso de la política

Puede asociar `AmazonDataZoneRedshiftGlueProvisioningPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de septiembre de 2023 a las 20:19 UTC
- Hora editada: 12 de marzo de 2024 a las 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```

```

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

```



```

    "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation:TagResource"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/DataZone*"
    ],
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : "AmazonDataZoneEnvironment"
      },
      "Null" : {
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
      }
    }
  },
  {
    "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/DataZone*"
    ]
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
    "Effect" : "Allow",
    "Action" : [
      "lakeformation:GetDataLakeSettings",
      "lakeformation:PutDataLakeSettings",
      "lakeformation:RevokePermissions",
      "lakeformation:ListPermissions",
      "glue:CreateDatabase",
      "glue:GetDatabase",
      "athena:GetWorkGroup",
      "logs:DescribeLogGroups",
      "redshift-serverless:GetNamespace",
      "redshift-serverless:GetWorkgroup",

```

```

    "redshift:DescribeClusters",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
    "lakeformation:ListResources"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue>DeleteDatabase"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "athena>DeleteWorkGroup"
  ],

```

```

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

```

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

```

```
    }  
  }  
} ]  
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

AmazonDataZoneRedshiftManageAccessRolePolicy es una [política AWS gestionada](#) que: Esta política otorga a Amazon DataZone permisos para publicar datos de Amazon Redshift en el catálogo. También otorga DataZone permisos a Amazon para conceder o revocar el acceso a los activos publicados en el catálogo de Amazon Redshift o Amazon Redshift Serverless.

Uso de la política

Puede asociar AmazonDataZoneRedshiftManageAccessRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de septiembre de 2023 a las 20:15 UTC
- Hora de edición: 16 de noviembre de 2023 a las 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```

    "Action" : "redshift-serverless:GetWorkgroup",
    "Resource" : [
      "arn:aws:redshift-serverless:*:*:workgroup/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "getNamespacePermission",
    "Effect" : "Allow",
    "Action" : "redshift-serverless:GetNamespace",
    "Resource" : [
      "arn:aws:redshift-serverless:*:*:namespace/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${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*"
  }
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDetectiveFullAccess

AmazonDetectiveFullAccess es una [política administrada por AWS](#) que: proporciona acceso total al servicio Amazon Detective y acceso limitado a las dependencias de la interfaz de usuario de la consola

Uso de esta política

Puede asociar AmazonDetectiveFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de abril de 2020 a las 17:57 UTC
- Hora de edición: 17 de mayo de 2023 a las 19:39 UTC

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

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings"
      ],
      "Resource" : "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDetectiveInvestigatorAccess

AmazonDetectiveInvestigatorAccess es una [política administrada de AWS](#) que proporciona a los investigadores acceso al servicio Amazon Detective y acceso limitado a las dependencias de la interfaz de usuario de la consola. Esta política otorga permiso para acceder a Detective con fines de investigación y acceso limitado por escrito a Guardduty.

Uso de esta política

Puede asociar AmazonDetectiveInvestigatorAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 17 de enero de 2023 a las 15:24 UTC
- Hora editada: 27 de noviembre de 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDataSourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",

```

```
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GuardDutyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "guardduty:ArchiveFindings",
    "guardduty:GetFindings",
    "guardduty:ListDetectors"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecurityHubPermissions",
  "Effect" : "Allow",
  "Action" : [
    "securityHub:GetFindings"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDetectiveMemberAccess

AmazonDetectiveMemberAccess es una [política administrada por AWS](#) que: proporciona a los miembros acceso al servicio Amazon Detective y acceso limitado a las dependencias de la interfaz de usuario de la consola.

Uso de esta política

Puede asociar `AmazonDetectiveMemberAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de enero de 2023 a las 15:16 UTC
- Hora de edición: 17 de enero de 2023 a las 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDetectiveOrganizationsAccess

AmazonDetectiveOrganizationsAccess es una [política administrada por AWS](#) que: proporciona a las organizaciones acceso para gestionar el administrador delegado de Amazon Detective y acceso limitado a las dependencias de la interfaz de usuario de la consola. Esto también concede permiso para crear un rol vinculado al servicio para Detective.

Uso de esta política

Puede asociar AmazonDetectiveOrganizationsAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de marzo de 2023 a las 15:20 UTC
- Hora de edición: 2 de marzo de 2023 a las 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com"
          ]
        }
      }
    }
  ],
  "Statement" : [
    {
      "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"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDetectiveServiceLinkedRolePolicy

AmazonDetectiveServiceLinkedRolePolicy es una [política administrada por AWS](#) que: permite a Amazon Detective realizar llamadas de servicio en su nombre

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2021 a las 19:47 UTC
- Hora de edición: 18 de noviembre de 2021 a las 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDevOpsGuruConsoleFullAccess

AmazonDevOpsGuruConsoleFullAccess es una [política administrada por AWS](#) que: otorga acceso total a la consola DevOps Guru.

Uso de esta política

Puede asociar AmazonDevOpsGuruConsoleFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de diciembre de 2021 a las 18:43 UTC
- Hora de edición: 25 de agosto de 2022 a las 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
{
  "Sid" : "DevOpsGuruFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "devops-guru:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudFormationListStacksAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchGetMetricDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SnsListTopicsAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SnsTopicOperations",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:GetTopicAttributes",
    "sns:SetTopicAttributes",
    "sns:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
},
}
```

```

{
  "Sid" : "DevOpsGuruSlrCreation",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "devops-guru.amazonaws.com"
    }
  }
},
{
  "Sid" : "DevOpsGuruSlrDeletion",
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
},
{
  "Sid" : "RDSDescribeDBInstancesAccess",
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PerformanceInsightsMetricsDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "pi:GetResourceMetrics",
    "pi:DescribeDimensionKeys"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchLogsFilterLogEventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:FilterLogEvents"
  ]
}

```

```
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDevOpsGuruFullAccess

AmazonDevOpsGuruFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon DevOps Guru.

Uso de esta política

Puede asociar AmazonDevOpsGuruFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2020 a las 16:38 UTC
- Hora de edición: 25 de agosto de 2022 a las 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ]
    }
  ]
}
```



```

    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SnsTopicOperations",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:GetTopicAttributes",
      "sns:SetTopicAttributes",
      "sns:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
  },
  {
    "Sid" : "DevOpsGuruSlrCreation",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "devops-guru.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "DevOpsGuruSlrDeletion",
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
  },
  {
    "Sid" : "RDSDescribeDBInstancesAccess",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
},

```

```
{
  "Sid" : "CloudWatchLogsFilterLogEventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:FilterLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
    }
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruOrganizationsAccess es una [política administrada por AWS](#) que: proporciona acceso para habilitar y administrar Amazon DevOps Guru dentro de una organización.

Uso de esta política

Puede asociar AmazonDevOpsGuruOrganizationsAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de noviembre de 2021 a las 23:50 UTC

- Hora de edición: 15 de noviembre de 2021 a las 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "arn:aws:organizations::*:"
    }
  ]
}
```

```
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "devops-guru.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDevOpsGuruReadOnlyAccess

AmazonDevOpsGuruReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a la consola Amazon DevOps Guru.

Uso de esta política

Puede asociar AmazonDevOpsGuruReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2020 a las 16:34 UTC
- Hora de edición: 25 de agosto de 2022 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
```

```
    "devops-guru:ListRecommendations",
    "devops-guru:SearchInsights",
    "devops-guru:StartCostEstimation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudFormationListStacksAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
},
{
  "Sid" : "CloudWatchGetMetricDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RDSDescribeDBInstancesAccess",
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchLogsFilterLogEventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:FilterLogEvents"
  ]
}
```

```
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
      }
    }
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDevOpsGuruServiceRolePolicy

AmazonDevOpsGuruServiceRolePolicy es una [política administrada por AWS](#) que: sirve como un rol vinculado a un servicio necesario para que Amazon DevOpsGuru pueda acceder a sus recursos.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de diciembre de 2020 a las 10:24 UTC
- Hora de edición: 10 de enero de 2023 a las 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
```



```

    "lambda:GetAccountSettings",
    "lambda:ListProvisionedConcurrencyConfigs",
    "lambda:ListAliases",
    "lambda:ListEventSourceMappings",
    "lambda:GetPolicy",
    "ec2:DescribeSubnets",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingPolicies",
    "sqs:GetQueueAttributes",
    "kinesis:DescribeStream",
    "kinesis:DescribeLimits",
    "dynamodb:DescribeTable",
    "dynamodb:DescribeLimits",
    "dynamodb:DescribeContinuousBackups",
    "dynamodb:DescribeStream",
    "dynamodb:ListStreams",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "rds:DescribeOptionGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeAccountAttributes",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "s3:GetBucketNotification",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketWebsite",
    "s3:GetIntelligentTieringConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowPutTargetsOnASpecificRule",

```

```

    "Effect" : "Allow",
    "Action" : [
      "events:PutTargets",
      "events:PutRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
  },
  {
    "Sid" : "AllowCreateOpsItem",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CreateOpsItem"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowAddTagsToOpsItem",
    "Effect" : "Allow",
    "Action" : [
      "ssm:AddTagsToResource"
    ],
    "Resource" : "arn:aws:ssm:*:*:opsitem/*"
  },
  {
    "Sid" : "AllowAccessOpsItem",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetOpsItem",
      "ssm:UpdateOpsItem"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
      }
    }
  },
  {
    "Sid" : "AllowCreateManagedRule",
    "Effect" : "Allow",
    "Action" : "events:PutRule",
    "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
  },
  {

```

```

    "Sid" : "AllowAccessManagedRule",
    "Effect" : "Allow",
    "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
},
{
    "Sid" : "AllowOtherOperationsOnManagedRule",
    "Effect" : "Allow",
    "Action" : [
        "events>DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
    "Condition" : {
        "StringEquals" : {
            "events:ManagedBy" : "devops-guru.amazonaws.com"
        }
    }
},
{
    "Sid" : "AllowTagBasedFilterLogEvents",
    "Effect" : "Allow",
    "Action" : [
        "logs:FilterLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
    }
},
{
    "Sid" : "AllowAPIGatewayGetIntegrations",
    "Effect" : "Allow",
    "Action" : "apigateway:GET",
    "Resource" : [
        "arn:aws:apigateway:*:*/restapis/????????????",

```

```
    "arn:aws:apigateway:*::/restapis/*/resources",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
  ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDMSCloudWatchLogsRole

AmazonDMSCloudWatchLogsRole es una [política administrada por AWS](#) que: proporciona acceso para cargar los registros de replicación del DMS a los registros de Cloudwatch de la cuenta del cliente.

Uso de esta política

Puede asociar AmazonDMSCloudWatchLogsRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de enero de 2016 a las 23:44 UTC
- Hora de edición: 23 de mayo de 2023 a las 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream"
      ],
    }
  ]
}
```

```
    "Resource" : [
      "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
      "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
    ],
  },
  {
    "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
      "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDMSRedshiftS3Role

AmazonDMSRedshiftS3Role es una [política administrada por AWS](#) que: proporciona acceso para gestionar la configuración de S3 para los puntos finales de Redshift para DMS.

Uso de esta política

Puede asociar AmazonDMSRedshiftS3Role a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2016 a las 17:05 UTC
- Hora de edición: 8 de julio de 2019 a las 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3>DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3>DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3>DeleteBucketPolicy"
      ],
    },
  ],
}
```

```
    "Resource" : "arn:aws:s3:::dms-*"  
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDMSVPCManagementRole

AmazonDMSVPCManagementRole es una [política administrada por AWS](#) que: proporciona acceso para administrar la configuración de VPC para las configuraciones administradas de clientes AWS

Uso de esta política

Puede asociar AmazonDMSVPCManagementRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de noviembre de 2015 a las 16:33 UTC
- Hora de edición: 23 de mayo de 2016 a las 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDocDB-ElasticServiceRolePolicy

AmazonDocDB-ElasticServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon DocumentDB-Elastic administrar los recursos AWS en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2022 a las 14:17 UTC
- Hora de edición: 30 de noviembre de 2022 a las 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}  
 ]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDocDBConsoleFullAccess

AmazonDocDBConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total para gestionar Amazon DocumentDB con compatibilidad con MongoDB mediante AWS Management Console. Tenga en cuenta que esta política también otorga acceso total para publicar sobre todos los temas de SNS de la cuenta. A su vez, concede permisos para crear y editar instancias de Amazon EC2 y configuraciones de VPC, y para ver y enumerar claves en Amazon KMS. Por último brinda acceso total a Amazon RDS y Amazon Neptune.

Uso de esta política

Puede asociar AmazonDocDBConsoleFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de enero de 2019 a las 20:37 UTC
- Hora de edición: 30 de noviembre de 2022 a las 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
    }
  }
}

```

```
}  
  }  
    }  
  ]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDocDBElasticFullAccess

AmazonDocDBElasticFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a los clústeres elásticos de Amazon DocumentDB y a otros permisos necesarios para sus dependencias, incluidos EC2, KMS, SecretsManager, CloudWatch e IAM.

Uso de esta política

Puede asociar AmazonDocDBElasticFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de junio de 2023 a las 13:51 UTC
- Hora de edición: 21 de junio de 2023 a las 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
        }
      }
    }
  ]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDocDBElasticReadOnlyAccess

AmazonDocDBElasticReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a las métricas de Amazon DocDB-Elastic y CloudWatch.

Uso de esta política

Puede asociar AmazonDocDBElasticReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de junio de 2023 a las 14:37 UTC
- Hora de edición: 21 de junio de 2023 a las 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "docdb-elastic:ListClusters",
      "docdb-elastic:GetCluster",
      "docdb-elastic:ListClusterSnapshots",
      "docdb-elastic:GetClusterSnapshot",
      "docdb-elastic:ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDocDBFullAccess

AmazonDocDBFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a Amazon DocumentDB con compatibilidad con MongoDB. Tenga en cuenta que esta política también otorga acceso total a las publicaciones sobre todos los temas de SNS de la cuenta, y brinda acceso total a Amazon RDS y Amazon Neptune.

Uso de esta política

Puede asociar `AmazonDocDBFullAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de enero de 2019 a las 20:21 UTC
- Hora de edición: 9 de enero de 2019 a las 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds>CreateDBCluster",
        "rds>CreateDBClusterParameterGroup",
        "rds>CreateDBClusterSnapshot",
        "rds>CreateDBInstance",
        "rds>CreateDBParameterGroup",
        "rds>CreateDBSubnetGroup",
        "rds>CreateEventSubscription",
```

```
"rds:DeleteDBCluster",
"rds:DeleteDBClusterParameterGroup",
"rds:DeleteDBClusterSnapshot",
"rds:DeleteDBInstance",
"rds:DeleteDBParameterGroup",
"rds:DeleteDBSubnetGroup",
"rds:DeleteEventSubscription",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
"rds:PromoteReadReplicaDBCluster",
"rds:RebootDBInstance",
"rds:RemoveRoleFromDBCluster",
"rds:RemoveSourceIdentifierFromSubscription",
```

```

    "rds:RemoveTagsFromResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "kms:ListAliases",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "sns:Publish"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "rds.amazonaws.com"
    }
  }
}

```



```
}  
  }  
    }  
  ]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDocDBReadOnlyAccess

AmazonDocDBReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon DocumentDB con compatibilidad con MongoDB. Tenga en cuenta que esta política también otorga acceso a los recursos de Amazon RDS y Amazon Neptune.

Uso de esta política

Puede asociar AmazonDocDBReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de enero de 2019 a las 20:30 UTC
- Hora de edición: 9 de enero de 2019 a las 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
}
```

```

{
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "kms:ListAliases",
    "kms:ListKeyPolicies"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
    "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
  ]
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDRSVPCManagement

AmazonDRSVPCManagement es una [política administrada por AWS](#) que: proporciona acceso para gestionar la configuración de VPC para las configuraciones de clientes gestionadas por Amazon

Uso de esta política

Puede asociar AmazonDRSVPCManagement a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de septiembre de 2015 a las 00:09 UTC
- Hora de edición: 2 de septiembre de 2015 a las 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
```

```
    "ec2:CreateSecurityGroup",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDynamoDBFullAccess

AmazonDynamoDBFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon DynamoDB a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonDynamoDBFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC

- Hora de edición: 29 de enero de 2021 a las 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Versión de la política

Versión de la política: v15 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline>DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
```

```

    "datapipeline:PutPipelineDefinition",
    "datapipeline:QueryObjects",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "iam:GetRole",
    "iam:ListRoles",
    "kms:DescribeKey",
    "kms:ListAliases",
    "sns:CreateTopic",
    "sns:DeleteTopic",
    "sns:ListSubscriptions",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:Unsubscribe",
    "sns:SetTopicAttributes",
    "lambda:CreateFunction",
    "lambda:ListFunctions",
    "lambda:ListEventSourceMappings",
    "lambda:CreateEventSourceMapping",
    "lambda>DeleteEventSourceMapping",
    "lambda:GetFunctionConfiguration",
    "lambda>DeleteFunction",
    "resource-groups:ListGroups",
    "resource-groups:ListGroupResources",
    "resource-groups:GetGroup",
    "resource-groups:GetGroupQuery",
    "resource-groups>DeleteGroup",
    "resource-groups:CreateGroup",
    "tag:GetResources",
    "kinesis:ListStreams",
    "kinesis:DescribeStream",
    "kinesis:DescribeStreamSummary"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : "cloudwatch:GetInsightRuleReport",
  "Effect" : "Allow",
  "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
},
{

```

```

    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "application-autoscaling.amazonaws.com",
          "application-autoscaling.amazonaws.com.cn",
          "dax.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "replication.dynamodb.amazonaws.com",
          "dax.amazonaws.com",
          "dynamodb.application-autoscaling.amazonaws.com",
          "contributorinsights.dynamodb.amazonaws.com",
          "kinesisreplication.dynamodb.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDynamoDBFullAccesswithDataPipeline

AmazonDynamoDBFullAccesswithDataPipeline es una [política administrada por AWS](#) que: está en vías de caducar. Consulte la documentación para obtener orientación: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>.

Proporciona acceso completo a Amazon DynamoDB, incluida la exportación e importación mediante Data Pipeline AWS a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonDynamoDBFullAccesswithDataPipeline a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 12 de noviembre de 2015 a las 2:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "cloudwatch:DescribeAlarmHistory",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "dynamodb:*",
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:ListSubscriptions",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:Unsubscribe",
    "sns:SetTopicAttributes"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Sid" : "DDBConsole"
},
{
  "Action" : [
    "lambda:*",
    "iam:ListRoles"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Sid" : "DDBConsoleTriggers"
},
{
  "Action" : [
    "datapipeline:*",
    "iam:ListRoles"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Sid" : "DDBConsoleImportExport"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRolePolicy",
    "iam:PassRole"
  ]
},

```

```

    "Resource" : [
      "*"
    ],
    "Sid" : "IAMEDPRoles"
  },
  {
    "Action" : [
      "ec2:CreateTags",
      "ec2:DescribeInstances",
      "ec2:RunInstances",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "elasticmapreduce:*",
      "datapipeline:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Sid" : "EMR"
  },
  {
    "Action" : [
      "s3:DeleteObject",
      "s3:Get*",
      "s3:List*",
      "s3:Put*"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "*"
    ],
    "Sid" : "S3"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonDynamoDBReadOnlyAccess

AmazonDynamoDBReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a Amazon DynamoDB a través de. AWS Management Console

Uso de la política

Puede asociar AmazonDynamoDBReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 20 de marzo de 2024 a las 15:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
```

```
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeAlarmsForMetric",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"cloudwatch:GetMetricData",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:QueryObjects",
"dynamodb:BatchGetItem",
"dynamodb:Describe*",
"dynamodb:List*",
"dynamodb: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*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonEBSCSIDriverPolicy

AmazonEBSCSIDriverPolicy es una [política administrada por AWS](#) que: IAM Policy que permite que la cuenta de servicio de controlador de CSI realice llamadas a servicios relacionados, como EC2, en su nombre.

Uso de esta política

Puede asociar AmazonEBSCSIDriverPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de abril de 2022 a las 17:24 UTC
- Hora de edición: 18 de noviembre de 2022 a las 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2ContainerRegistryFullAccess

AmazonEC2ContainerRegistryFullAccess es una [política administrada por AWS](#) que proporciona acceso administrativo a los recursos de Amazon ECR.

Uso de esta política

Puede asociar AmazonEC2ContainerRegistryFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de diciembre de 2015 a las 17:06 UTC
- Hora de edición: 5 de diciembre de 2020 a las 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.ecr.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2ContainerRegistryPowerUser

AmazonEC2ContainerRegistryPowerUser es una [política administrada por AWS](#) que: proporciona acceso total a los repositorios de Amazon EC2 Container Registry, pero no permite la eliminación de repositorios ni los cambios de política.

Uso de esta política

Puede asociar AmazonEC2ContainerRegistryPowerUser a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de diciembre de 2015 a las 17:05 UTC
- Hora de edición: 10 de diciembre de 2019 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Action" : [
  "ecr:GetAuthorizationToken",
  "ecr:BatchCheckLayerAvailability",
  "ecr:GetDownloadUrlForLayer",
  "ecr:GetRepositoryPolicy",
  "ecr:DescribeRepositories",
  "ecr:ListImages",
  "ecr:DescribeImages",
  "ecr:BatchGetImage",
  "ecr:GetLifecyclePolicy",
  "ecr:GetLifecyclePolicyPreview",
  "ecr:ListTagsForResource",
  "ecr:DescribeImageScanFindings",
  "ecr:InitiateLayerUpload",
  "ecr:UploadLayerPart",
  "ecr:CompleteLayerUpload",
  "ecr:PutImage"
],
"Resource" : "*"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2ContainerRegistryReadOnly

AmazonEC2ContainerRegistryReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a los repositorios de Amazon EC2 Container Registry.

Uso de esta política

Puede asociar AmazonEC2ContainerRegistryReadOnly a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de diciembre de 2015 a las 17:04 UTC
- Hora de edición: 10 de diciembre de 2019 a las 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2ContainerServiceAutoscaleRole

AmazonEC2ContainerServiceAutoscaleRole es una [política administrada por AWS](#) que permite el escalado automático de tareas para Amazon EC2 Container Service

Uso de esta política

Puede asociar AmazonEC2ContainerServiceAutoscaleRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de mayo de 2016 a las 23:25 UTC
- Hora de edición: 5 de febrero de 2018 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs:DescribeServices",
      "ecs:UpdateService"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms",
      "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2ContainerServiceEventsRole

AmazonEC2ContainerServiceEventsRole es una [política administrada por AWS](#) que: permite eventos de CloudWatch para EC2 Container Service

Uso de esta política

Puede asociar `AmazonEC2ContainerServiceEventsRole` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 30 de mayo de 2017 a las 16:51 UTC
- Hora de edición: 6 de marzo de 2023 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ecs-tasks.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ecs:TagResource",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "RunTask"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2ContainerServiceforEC2Role

AmazonEC2ContainerServiceforEC2Role es una [política administrada por AWS](#) que: Política predeterminada para el rol de Amazon EC2 para Amazon EC2 Container Service.

Uso de esta política

Puede asociar AmazonEC2ContainerServiceforEC2Role a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de marzo de 2015 a las 18:45 UTC
- Hora de edición: 06 de marzo de 2023 a las 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ecs:TagResource",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "CreateCluster",
          "RegisterContainerInstance"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2ContainerServiceRole

AmazonEC2ContainerServiceRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio de Amazon ECS.

Uso de esta política

Puede asociar AmazonEC2ContainerServiceRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio

- Hora de creación: 9 de abril de 2015 a las 16:14 UTC
- Hora de edición: 11 de agosto de 2016 a las 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2FullAccess

AmazonEC2FullAccess es una [política administrada por AWS](#) que: brinda acceso total a Amazon EC2 a través de la AWS Management Console.

Uso de esta política

Puede asociar AmazonEC2FullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 27 de noviembre de 2018 a las 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : "elasticloadbalancing:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "autoscaling:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "autoscaling.amazonaws.com",
          "ec2scheduled.amazonaws.com",
          "elasticloadbalancing.amazonaws.com",
          "spot.amazonaws.com",
          "spotfleet.amazonaws.com",
          "transitgateway.amazonaws.com"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2ReadOnlyAccess

AmazonEC2ReadOnlyAccess es una [política AWS gestionada](#) que: proporciona acceso de solo lectura a Amazon EC2 a través del AWS Management Console

Uso de la política

Puede asociar AmazonEC2ReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 14 de febrero de 2024 a las 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonEC2RoleforAWSCodeDeploy

AmazonEC2RoleforAWSCodeDeploy es una [política administrada por AWS](#) que: proporciona acceso EC2 al bucket S3 para descargar la revisión. El agente CodeDeploy requiere esta función en instancias EC2.

Uso de esta política

Puede asociar AmazonEC2RoleforAWSCodeDeploy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio

- Hora de creación: 19 de mayo de 2015 a las 18:10 UTC
- Hora de edición: 20 de marzo de 2017 a las 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2RoleforAWSCodeDeployLimited

AmazonEC2RoleforAWSCodeDeployLimited es una [política administrada por AWS](#) que proporciona acceso limitado EC2 al bucket S3 para descargar la revisión. El agente CodeDeploy requiere esta función en instancias EC2.

Uso de esta política

Puede asociar AmazonEC2RoleforAWSCodeDeployLimited a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de agosto de 2020 a las 17:55 UTC
- Hora de edición: 20 de enero de 2022 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ]
    }
  ],
}
```

```
    "Resource" : "arn:aws:s3:::*/CodeDeploy/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2RoleforDataPipelineRole

AmazonEC2RoleforDataPipelineRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio de Amazon EC2 para Data Pipeline.

Uso de esta política

Puede asociar AmazonEC2RoleforDataPipelineRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio

- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 22 de febrero de 2016 a las 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
        "elasticmapreduce:ModifyInstanceGroups",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}  
  ]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2RoleforSSM

AmazonEC2RoleforSSM es una [política administrada por AWS](#) que: está en vías de quedar obsoleta. Utilice la política AmazonSSMManagedInstanceCore para habilitar AWS la funcionalidad principal del servicio de administración de sistemas en las instancias EC2. Para obtener más información, consulte <https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>

Uso de esta política

Puede asociar AmazonEC2RoleforSSM a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de mayo de 2015 a las 17:48 UTC
- Hora de edición: 24 de enero de 2019 a las 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
```

```

    "ec2messages:DeleteMessage",
    "ec2messages:FailMessage",
    "ec2messages:GetEndpoint",
    "ec2messages:GetMessages",
    "ec2messages:SendReply"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstanceStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ds:CreateComputer",
    "ds:DescribeDirectories"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [

```



```
    "s3:GetBucketLocation",
    "s3:PutObject",
    "s3:GetObject",
    "s3:GetEncryptionConfiguration",
    "s3:AbortMultipartUpload",
    "s3:ListMultipartUploadParts",
    "s3:ListBucket",
    "s3:ListBucketMultipartUploads"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2RolePolicyForLaunchWizard

AmazonEC2RolePolicyForLaunchWizard es una [política administrada por AWS](#) que: Política administrada para el rol de servicio Amazon LaunchWizard para EC2

Uso de esta política

Puede asociar AmazonEC2RolePolicyForLaunchWizard a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de noviembre de 2019 a las 08:05 UTC
- Hora de edición: 16 de mayo de 2022 a las 21:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAddresses",
    "ec2:AssociateAddress",
    "ec2:DescribeInstances",
    "ec2:DescribeImages",
    "ec2:DescribeRegions",
    "ec2:DescribeVolumes",
    "ec2:DescribeRouteTables",
    "ec2:ModifyInstanceAttribute",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:PutMetricData",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "LaunchWizardResourceGroupID",
        "LaunchWizardApplicationType"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectTagging",
    "s3:GetBucketLocation",
    "logs:PutLogEvents",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams"
  ]
}
```

```

    ],
    "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
    ]
},
{
    "Effect" : "Allow",
    "Action" : "logs:Create*",
    "Resource" : "arn:aws:logs:*:*:*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb>DeleteTable",
        "dynamodb>CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",

```

```

    "dynamodb:UpdateTable"
  ],
  "Resource" : [
    "arn:aws:s3:::launchwizard*",
    "arn:aws:dynamodb:*:*:table/LaunchWizard*",
    "arn:aws:sqs:*:*:LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/LaunchWizardApplicationType" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand",
    "ssm:GetDocument"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeFileSystems",
    "fsx:ListTagsForResource",
    "fsx:DescribeStorageVirtualMachines"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "LaunchWizard*"
    }
  }
}
]

```

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2SpotFleetAutoscaleRole

AmazonEC2SpotFleetAutoscaleRole es una [política administrada por AWS](#) que: habilita el escalado automático para la flota de spot de Amazon EC2

Uso de esta política

Puede asociar AmazonEC2SpotFleetAutoscaleRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de agosto de 2016 a las 18:27 UTC
- Hora de edición: 18 de febrero de 2019 a las 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEC2SpotFleetTaggingRole

AmazonEC2SpotFleetTaggingRole es una [política administrada por AWS](#) que: permite a EC2 Spot Fleet solicitar, cancelar y etiquetar instancias puntuales en su nombre.

Uso de esta política

Puede asociar AmazonEC2SpotFleetTaggingRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de junio de 2017 a las 18:19 UTC
- Hora de edición: 23 de abril de 2020 a las 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:DescribeSubnets",
      "ec2:RequestSpotInstances",
      "ec2:TerminateInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:CreateTags",
      "ec2:RunInstances"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn"
        ]
      }
    },
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets"
    ]
  }
]
```

```
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:*/*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonECS_FullAccess

AmazonECS_FullAccess es una [política administrada por AWS](#) que: proporciona acceso administrativo a los recursos de Amazon ECS y permite características ECS a través del acceso a otros recursos de servicios AWS, que incluye VPC, grupos de escalado automático y pilas de CloudFormation.

Uso de esta política

Puede asociar AmazonECS_FullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de noviembre de 2017 a las 21:36 UTC
- Hora de edición: 4 de enero de 2023 a las 16:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Versión de la política

Versión de la política: v20 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "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"
      ]
    }
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurityes una [política AWS gestionada](#) que: proporciona acceso administrativo a Private Certificate Authority, AWS Secrets Manager y otros elementos Servicios de AWS necesarios para gestionar las funciones TLS de ECS Service Connect en su nombre.

Uso de la política

Puede asociar

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de enero de 2024 a las 20:08 UTC
- Hora editada: 19 de enero de 2024 a las 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        }
      },
      "StringEquals" : {
```

```

        "aws:RequestTag/AmazonECSTag" : "true",
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
},
{
    "Sid" : "TagOnCreateSecret",
    "Effect" : "Allow",
    "Action" : "secretsmanager:TagResource",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
    "Condition" : {
        "ArnLike" : {
            "aws:RequestTag/AmazonECSTag" : [
                "arn:aws:ecs:*:*:service/*/*",
                "arn:aws:ecs:*:*:task-set/*/*"
            ]
        },
        "StringEquals" : {
            "aws:RequestTag/AmazonECSTag" : "true",
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "RotateTLSCertificateSecret",
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
    "Condition" : {
        "StringEquals" : {
            "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{

```

```

    "Sid" : "ManagePrivateCertificateAuthority",
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:GetCertificate",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:DescribeCertificateAuthority"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AmazonECSManaged" : "true"
      }
    }
  },
  {
    "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:IssueCertificate"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AmazonECSManaged" : "true",
        "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonECSInfrastructureRolePolicyForVolumes

AmazonECSInfrastructureRolePolicyForVolumes es una [política AWS administrada](#) que proporciona acceso a otros recursos de AWS servicio necesarios para administrar los volúmenes asociados a las cargas de trabajo de ECS en su nombre.

Uso de la política

Puede asociar AmazonECSInfrastructureRolePolicyForVolumes a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de enero de 2024 a las 22:56 UTC
- Hora editada: 10 de enero de 2024 a las 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
```

```
    "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
  },
  "StringEquals" : {
    "aws:RequestTag/AmazonECSManaged" : "true"
  }
},
{
  "Sid" : "TagOnCreateVolume",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "ArnLike" : {
      "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
    },
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVolume",
      "aws:RequestTag/AmazonECSManaged" : "true"
    }
  }
},
{
  "Sid" : "DescribeVolumesForLifecycle",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVolumes",
    "ec2:DescribeAvailabilityZones"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ManageEBSVolumeLifecycle",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSManaged" : "true"
    }
  }
}
```

```

    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonECSServiceRolePolicy

AmazonECSServiceRolePolicy es una [política administrada de AWS](#) que permite a Amazon ECS administrar su clúster.

Uso de esta política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de octubre de 2017 a la 01:18 UTC
- Hora editada: 4 de diciembre de 2023, 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
```

```

    "elasticloadbalancing:RegisterTargets",
    "route53:ChangeResourceRecordSets",
    "route53:CreateHealthCheck",
    "route53>DeleteHealthCheck",
    "route53:Get*",
    "route53:List*",
    "route53:UpdateHealthCheck",
    "servicediscovery:DeregisterInstance",
    "servicediscovery:Get*",
    "servicediscovery:List*",
    "servicediscovery:RegisterInstance",
    "servicediscovery:UpdateInstanceCustomHealthStatus"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AutoScaling",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AutoScalingManagement",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DeletePolicy",
    "autoscaling:PutScalingPolicy",
    "autoscaling:SetInstanceProtection",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:PutLifecycleHook",
    "autoscaling>DeleteLifecycleHook",
    "autoscaling:CompleteLifecycleAction",
    "autoscaling:RecordLifecycleActionHeartbeat"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "autoscaling:ResourceTag/AmazonECSManaged" : "false"
    }
  }
}
},
{

```



```

    "Sid" : "AutoScalingPlanManagement",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling-plans:CreateScalingPlan",
      "autoscaling-plans>DeleteScalingPlan",
      "autoscaling-plans:DescribeScalingPlans",
      "autoscaling-plans:DescribeScalingPlanResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EventBridge",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
  },
  {
    "Sid" : "EventBridgeRuleManagement",
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule",
      "events:PutTargets"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "events:ManagedBy" : "ecs.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CWAlarmManagement",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch>DeleteAlarms",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
  },
  {

```

```

    "Sid" : "ECSTagging",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
    "Sid" : "CWLogGroupManagement",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
},
{
    "Sid" : "CWLogStreamManagement",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
},
{
    "Sid" : "ExecuteCommandSessionManagement",
    "Effect" : "Allow",
    "Action" : [
        "ssm:DescribeSessions"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ExecuteCommand",
    "Effect" : "Allow",
    "Action" : [
        "ssm:StartSession"
    ],
    "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
    ]
}

```

```
]
},
{
  "Sid" : "CloudMapResourceCreation",
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:CreateHttpNamespace",
    "servicediscovery:CreateService"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AmazonECSManaged"
      ]
    }
  }
},
{
  "Sid" : "CloudMapResourceTagging",
  "Effect" : "Allow",
  "Action" : "servicediscovery:TagResource",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AmazonECSManaged" : "*"
    }
  }
},
{
  "Sid" : "CloudMapResourceDeletion",
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:DeleteService"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonECSManaged" : "false"
    }
  }
},
{
  "Sid" : "CloudMapResourceDiscovery",
```

```
    "Effect" : "Allow",
    "Action" : [
      "servicediscovery:DiscoverInstances",
      "servicediscovery:DiscoverInstancesRevision"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonECSTaskExecutionRolePolicy

AmazonECSTaskExecutionRolePolicy es una [política administrada por AWS](#) que: proporciona acceso a otros recursos de servicio AWS necesarios para ejecutar tareas de Amazon ECS

Uso de esta política

Puede asociar AmazonECSTaskExecutionRolePolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 16 de noviembre de 2017 a las 18:48 UTC
- Hora de edición: 16 de noviembre de 2017 a las 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEFSCSIDriverPolicy

AmazonEFSCSIDriverPolicy es una [política administrada por AWS](#) que: proporciona acceso de administración a los recursos de EFS y acceso de lectura a EC2

Uso de esta política

Puede asociar `AmazonEFSCSIDriverPolicy` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de julio de 2023 a las 20:10 UTC
- Hora de edición: 25 de julio de 2023 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "efs.csi.aws.com/cluster"
      }
    }
  },
  {
    "Sid" : "AllowTagNewAccessPoints",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "elasticfilesystem:CreateAction" : "CreateAccessPoint"
      },
      "Null" : {
        "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "efs.csi.aws.com/cluster"
      }
    }
  },
  {
    "Sid" : "AllowDeleteAccessPoint",
    "Effect" : "Allow",
    "Action" : "elasticfilesystem:DeleteAccessPoint",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKS_CNI_Policy

AmazonEKS_CNI_Policy es una [política AWS gestionada](#) que: Esta política proporciona al complemento CNI de Amazon VPC (amazon-vpc-cni-k8s) los permisos que necesita para modificar la configuración de la dirección IP en los nodos de trabajo de EKS. Este conjunto de permisos permite al CNI enumerar, describir y modificar las interfaces de Elastic Network en su nombre. Puede encontrar más información sobre el complemento CNI de AWS VPC aquí: <https://github.com/aws/8s-amazon-vpc-cni-k>

Uso de la política

Puede asociar AmazonEKS_CNI_Policy a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 27 de mayo de 2018 a las 21:07 UTC
- Hora editada: 4 de marzo de 2024 a las 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonEKSClusterPolicy

AmazonEKSClusterPolicy es una [política administrada por AWS](#) que: proporciona a Kubernetes los permisos que necesita para gestionar los recursos en su nombre. Kubernetes requiere permisos EC2:CreateTags para colocar información de identificación en los recursos de EC2, incluidas, entre otras, las instancias, los grupos de seguridad y las interfaces de red elásticas.

Uso de esta política

Puede asociar AmazonEKSClusterPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2018 a las 21:06 UTC
- Hora de edición: 7 de febrero de 2023 a las 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSCredentialsServiceRolePolicy

AmazonEKSCredentialsServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon EKS administrar los recursos AWS del conector EKS

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de septiembre de 2021 a las 20:31 UTC
- Hora de edición: 4 de septiembre de 2021 a las 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCredentialsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMServices",
      "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"
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSFargatePodExecutionRolePolicy

AmazonEKSFargatePodExecutionRolePolicy es una [política administrada por AWS](#) que proporciona acceso a otros recursos de servicio AWS necesarios para ejecutar pods de Amazon EKS en Fargate AWS

Uso de esta política

Puede asociar AmazonEKSFargatePodExecutionRolePolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de noviembre de 2019 a las 04:34 UTC

- Hora de edición: 22 de noviembre de 2019 a las 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSFargateServiceRolePolicy

AmazonEKSFargateServiceRolePolicy es una [política administrada por AWS](#) que: concede los permisos necesarios a Amazon EKS para ejecutar tareas de Fargate

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de noviembre de 2019 a las 04:36 UTC
- Hora de edición: 22 de noviembre de 2019 a las 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
```

```
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeRouteTables"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSLocalOutpostClusterPolicy

AmazonEKSLocalOutpostClusterPolicy es una [política administrada por AWS](#) que: proporciona permisos a las instancias del plano de control del clúster local de EKS que se ejecutan en su cuenta para administrar los recursos en su nombre.

Uso de esta política

Puede asociar AmazonEKSLocalOutpostClusterPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de agosto de 2022 a las 21:56 UTC
- Hora de edición: 17 de octubre de 2022 a las 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSLocalOutpostServiceRolePolicy

AmazonEKSLocalOutpostServiceRolePolicy es una [política administrada por AWS](#) que permite a Amazon EKS Local llamar a los servicios AWS en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de agosto de 2022 a las 21:53 UTC
- Hora de edición: 24 de octubre de 2022 a las 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeRouteTables",
      "ec2:DescribeAddresses",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribePlacementGroups"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:subnet/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : [

```

```

    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",

```

```

    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:placement-group*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:TerminateInstances",
    "ec2:GetConsoleOutput"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:instance*"
  ],
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "kubernetes.io/cluster/*",
        "eks*"
      ]
    }
  },
  "StringEquals" : {
    "ec2:CreateAction" : [
      "CreateNetworkInterface",
      "CreateSecurityGroup",

```



```

        "RunInstances"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : [
          "kubernetes.io/cluster/*",
          "eks*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "secretsmanager:DeleteSecret",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",

```

```
    "Action" : "secretsmanager:DescribeSecret",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource" : "arn:aws:iam:*:*:instance-profile/eks-local-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ssm:resourceTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/AmazonEKS-ControlPlaneInstanceProxy"
  },
  {
```

```
    "Effect" : "Allow",
    "Action" : [
      "ssm:ResumeSession",
      "ssm:TerminateSession"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "outposts:GetOutpost"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSServicePolicy

AmazonEKSServicePolicy es una [política administrada por AWS](#) que: permite a Amazon Elastic Container Service for Kubernetes crear y administrar los recursos necesarios para operar clústeres de EKS.

Uso de esta política

Puede asociar AmazonEKSServicePolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2018 a las 21:08 UTC
- Hora de edición: 27 de mayo de 2020 a las 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion"
      ],
      "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"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSServiceRolePolicy

AmazonEKSServiceRolePolicy es una [política administrada por AWS](#) que: requiere una función vinculada al servicio para que Amazon EKS pueda llamar a los servicios AWS en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de febrero de 2020 a las 20:10 UTC
- Hora de edición: 27 de mayo de 2020 a las 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```


Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSVPCResourceController

AmazonEKSVPCResourceController es una [política administrada por AWS](#) que: es utilizada por el controlador de recursos de VPC para administrar el ENI y las IP de los nodos de trabajo.

Uso de esta política

Puede asociar AmazonEKSVPCResourceController a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de agosto de 2020 a las 00:55 UTC
- Hora de edición: 12 de agosto de 2020 a las 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
```

```

    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface",
      "ec2:DetachNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2>DeleteNetworkInterface",
      "ec2:AttachNetworkInterface",
      "ec2:UnassignPrivateIpAddresses",
      "ec2:AssignPrivateIpAddresses"
    ],
    "Resource" : "*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEKSWorkerNodePolicy

AmazonEKSWorkerNodePolicy es una [política administrada de AWS](#) que permite que los nodos de trabajo de Amazon EKS se conecten a los clústeres de Amazon EKS.

Uso de esta política

Puede asociar AmazonEKSWorkerNodePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 27 de mayo de 2018 a las 21:09 UTC
- Hora editada: 27 de noviembre de 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSEKSWorkerNodePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElastiCacheFullAccess

AmazonElastiCacheFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a Amazon ElastiCache a través deAWS Management Console.

Uso de la política

Puede asociar AmazonElastiCacheFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 28 de noviembre de 2023 a las 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

"Statement" : [
  {
    "Sid" : "ElastiCacheManagementActions",
    "Effect" : "Allow",
    "Action" : "elasticache:*",
    "Resource" : "*"
  },
  {
    "Sid" : "CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/
AWSServiceRoleForElastiCache",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "elasticache.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CreateVPCEndpoints",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : "arn:aws:ec2::*:vpc-endpoint/*",
    "Condition" : {
      "StringLike" : {
        "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
      }
    }
  },
  {
    "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint"
    ],
    "NotResource" : "arn:aws:ec2::*:vpc-endpoint/*"
  },
  {
    "Sid" : "TagVPCEndpointsOnCreation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
  },

```

```

    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint",
        "aws:RequestTag/AmazonElasticCacheManaged" : "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" : "*"
}
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElastiCacheReadOnlyAccess

AmazonElastiCacheReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon ElastiCache a través de AWS Management Console

Uso de esta política

Puede asociar AmazonElastiCacheReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticContainerRegistryPublicFullAccess

AmazonElasticContainerRegistryPublicFullAccess es una [política administrada por AWS](#) que: proporciona acceso administrativo a los recursos públicos de Amazon ECR

Uso de esta política

Puede asociar AmazonElasticContainerRegistryPublicFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 1 de diciembre de 2020 a las 17:25 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticContainerRegistryPublicPowerUser

AmazonElasticContainerRegistryPublicPowerUser es una [política administrada por AWS](#) que: proporciona acceso total a los repositorios públicos de Amazon ECR, pero no permite la eliminación de los repositorios ni los cambios en la política.

Uso de esta política

Puede asociar AmazonElasticContainerRegistryPublicPowerUser a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2020 a las 16:16 UTC
- Hora de edición: 1 de diciembre de 2020 a las 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
```

```
    "ecr-public:DescribeRepositories",
    "ecr-public:DescribeRegistries",
    "ecr-public:DescribeImages",
    "ecr-public:DescribeImageTags",
    "ecr-public:GetRepositoryCatalogData",
    "ecr-public:GetRegistryCatalogData",
    "ecr-public:InitiateLayerUpload",
    "ecr-public:UploadLayerPart",
    "ecr-public:CompleteLayerUpload",
    "ecr-public:PutImage"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticContainerRegistryPublicReadOnly

AmazonElasticContainerRegistryPublicReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a los repositorios públicos de Amazon ECR.

Uso de esta política

Puede asociar AmazonElasticContainerRegistryPublicReadOnly a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2020 a las 17:27 UTC

- Hora de edición: 1 de diciembre de 2020 a las 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticFileSystemClientFullAccess

AmazonElasticFileSystemClientFullAccess es una [política administrada por AWS](#) que proporciona acceso de cliente raíz a un sistema de archivos Amazon EFS

Uso de esta política

Puede asociar AmazonElasticFileSystemClientFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de enero de 2020 a las 16:27 UTC
- Hora de edición: 13 de enero de 2020 a las 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticFileSystemClientReadOnlyAccess

AmazonElasticFileSystemClientReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de cliente de solo lectura a un sistema de archivos Amazon EFS

Uso de esta política

Puede asociar AmazonElasticFileSystemClientReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de enero de 2020 a las 16:24 UTC
- Hora de edición: 13 de enero de 2020 a las 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticFileSystemClientReadWriteAccess

AmazonElasticFileSystemClientReadWriteAccess es una [política administrada por AWS](#) que: proporciona acceso de cliente de lectura y escritura a un sistema de archivos Amazon EFS

Uso de esta política

Puede asociar AmazonElasticFileSystemClientReadWriteAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de enero de 2020 a las 16:21 UTC
- Hora de edición: 13 de enero de 2020 a las 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticFileSystemFullAccess

AmazonElasticFileSystemFullAccess es una [política administrada de AWS](#) que proporciona acceso total a Amazon EFS a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonElasticFileSystemFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 27 de mayo de 2015 a las 16:22 UTC
- Hora editada: 28 de noviembre de 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticFileSystemReadOnlyAccess

AmazonElasticFileSystemReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a Amazon EFS a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonElasticFileSystemReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 27 de mayo de 2015 a las 16:25 UTC
- Hora de edición: 10 de enero de 2022 a las 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticFileSystemServiceRolePolicy

AmazonElasticFileSystemServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon Elastic File System gestionar los recursos AWS en su nombre

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de noviembre de 2019 a las 16:52 UTC
- Hora de edición: 10 de enero de 2022 a las 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```

    "backup:CreateBackupPlan",
    "backup:CreateBackupSelection"
  ],
  "Resource" : [
    "arn:aws:backup:*:*:backup-plan:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "backup.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:CreateReplicationConfiguration",
    "elasticfilesystem:DescribeReplicationConfigurations",
    "elasticfilesystem>DeleteReplicationConfiguration"
  ],

```



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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticFileSystemsUtils

AmazonElasticFileSystemsUtils es una [política administrada por AWS](#) que: permite a los clientes utilizar Systems Manager AWS para gestionar automáticamente el paquete de utilidades de Amazon EFS (amazon-efs-utils) en sus instancias EC2 y utilizar CloudWatchLog para recibir notificaciones de éxito o error al montar el sistema de archivos EFS.

Uso de esta política

Puede asociar AmazonElasticFileSystemsUtils a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de septiembre de 2020 a las 15:16 UTC
- Hora de edición: 29 de septiembre de 2020 a las 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
```

```
    "ec2messages:GetMessages",
    "ec2messages:SendReply"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeMountTargets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAvailabilityZones"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:PutLogEvents",
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups",
    "logs:CreateLogStream",
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "*"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticMapReduceEditorsRole

AmazonElasticMapReduceEditorsRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio Amazon Elastic MapReduce Editors.

Uso de esta política

Puede asociar AmazonElasticMapReduceEditorsRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 16 de noviembre de 2018, 21:55 UTC
- Hora de edición: 09 de febrero de 2023 a las 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
```

```

    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:DescribeSecurityGroups",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2:DescribeNetworkInterfaces",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "elasticmapreduce:ListInstances",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListSteps"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws:elasticmapreduce:editor-id",
        "aws:elasticmapreduce:job-flow-id"
      ]
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticMapReduceforAutoScalingRole

AmazonElasticMapReduceforAutoScalingRole es una [política administrada por AWS](#) que: está predeterminada para Amazon Elastic MapReduce para escalado automático. Rol para permitir que el escalado automático añada y elimine instancias de su clúster de EMR.

Uso de esta política

Puede asociar AmazonElasticMapReduceforAutoScalingRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de noviembre de 2016 a las 01:09 UTC
- Hora de edición: 18 de noviembre de 2016 a las 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
```

```
    "elasticmapreduce:ModifyInstanceGroups"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticMapReduceforEC2Role

AmazonElasticMapReduceforEC2Role es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio Amazon Elastic MapReduce para EC2.

Uso de esta política

Puede asociar AmazonElasticMapReduceforEC2Role a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 11 de agosto de 2017 a las 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis>DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
        "kinesis:PutRecord",
        "kinesis:SplitShard",
        "rds:Describe*",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue>DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue>DeleteTable",
```



```
"glue:GetTable",
"glue:GetTables",
"glue:GetTableVersions",
"glue:CreatePartition",
"glue:BatchCreatePartition",
"glue:UpdatePartition",
"glue>DeletePartition",
"glue:BatchDeletePartition",
"glue:GetPartition",
"glue:GetPartitions",
"glue:BatchGetPartition",
"glue:CreateUserDefinedFunction",
"glue:UpdateUserDefinedFunction",
"glue>DeleteUserDefinedFunction",
"glue:GetUserDefinedFunction",
"glue:GetUserDefinedFunctions"
]
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticMapReduceFullAccess

AmazonElasticMapReduceFullAccess es una [política administrada por AWS](#) que: está en vías de caducar. Consulte la documentación para obtener orientación: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Proporciona acceso completo a Amazon Elastic MapReduce y a los servicios subyacentes que requiere, como EC2 y S3

Uso de esta política

Puede asociar `AmazonElasticMapReduceFullAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 11 de octubre de 2019 a las 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2>DeleteRoute",
        "ec2>DeleteTags",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
```

```

    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSpotPriceHistory",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DescribeRouteTables",
    "ec2:DescribeNetworkAcls",
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyImageAttribute",
    "ec2:ModifyInstanceAttribute",
    "ec2:RequestSpotInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "elasticmapreduce:*",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:List*",
    "s3:*",
    "sdb:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [
        "elasticmapreduce.amazonaws.com",
        "elasticmapreduce.amazonaws.com.cn"
      ]
    }
  }
}
]

```

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticMapReducePlacementGroupPolicy

AmazonElasticMapReducePlacementGroupPolicy es una [política administrada por AWS](#) que: permite a EMR crear, describir y eliminar grupos de ubicación de EC2.

Uso de esta política

Puede asociar AmazonElasticMapReducePlacementGroupPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de septiembre de 2020 a las 00:37 UTC
- Hora de edición: 29 de septiembre de 2020 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups"
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticMapReduceReadOnlyAccess

AmazonElasticMapReduceReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Elastic MapReduce a través de AWS Management Console.

Uso de esta política

Puede asociar `AmazonElasticMapReduceReadOnlyAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 29 de julio de 2020 a las 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticMapReduceRole

AmazonElasticMapReduceRole es una [política administrada por AWS](#) que: está en vías de caducar. Consulte la documentación para obtener orientación: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Política predeterminada para el rol de servicio Amazon Elastic MapReduce.

Uso de esta política

Puede asociar AmazonElasticMapReduceRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 24 de junio de 2020 a las 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
```



```

    "ec2:ModifyImageAttribute",
    "ec2:ModifyInstanceAttribute",
    "ec2:RequestSpotInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "ec2>DeleteVolume",
    "ec2:DescribeVolumeStatus",
    "ec2:DescribeVolumes",
    "ec2:DetachVolume",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListInstanceProfiles",
    "iam:ListRolePolicies",
    "iam:PassRole",
    "s3:CreateBucket",
    "s3:Get*",
    "s3:List*",
    "sdb:BatchPutAttributes",
    "sdb:Select",
    "sqs:CreateQueue",
    "sqs>Delete*",
    "sqs:GetQueue*",
    "sqs:PurgeQueue",
    "sqs:ReceiveMessage",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DescribeAlarms",
    "cloudwatch>DeleteAlarms",
    "application-autoscaling:RegisterScalableTarget",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling>DeleteScalingPolicy",
    "application-autoscaling:Describe*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "spot.amazonaws.com"
    }
  }
}

```

```
    }  
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticsearchServiceRolePolicy

AmazonElasticsearchServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon Elasticsearch Service acceder a otros servicios de AWS, como las API de redes de EC2, en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de julio de 2017 a las 00:15 UTC
- Hora de edición: 23 de octubre de 2023 a las 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    }
  ]
}
```

```
},
{
  "Sid" : "Stmt1480452973198",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "Stmt1480452973199",
  "Effect" : "Allow",
  "Action" : "ec2:CreateVpcEndpoint",
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/OpenSearchManaged" : "true"
    }
  }
},
{
  "Sid" : "Stmt1480452973200",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/OpenSearchManaged" : "true"
    }
  }
},
{
  "Sid" : "Stmt1480452973201",
  "Effect" : "Allow",
  "Action" : [
```

```

    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973149",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973150",
  "Effect" : "Allow",
  "Action" : [
    "ec2:UnAssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973202",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticTranscoder_FullAccess

AmazonElasticTranscoder_FullAccess es una [política administrada por AWS](#) que: otorga a los usuarios acceso total a Elastic Transcoder y a los servicios asociados necesarios para la funcionalidad completa de Elastic Transcoder.

Uso de esta política

Puede asociar AmazonElasticTranscoder_FullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de abril de 2018 a las 18:59 UTC
- Hora de edición: 10 de junio de 2019 a las 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
    },
  ],
}
```

```
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "elastictranscoder.amazonaws.com"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticTranscoder_JobsSubmitter

AmazonElasticTranscoder_JobsSubmitter es una [política administrada por AWS](#) que: concede a los usuarios permiso para cambiar los ajustes preestablecidos, enviar trabajos y ver la configuración de Elastic Transcoder. Esta política también otorga acceso de solo lectura a algunos otros servicios necesarios para usar la consola de Elastic Transcode, como S3, IAM y SNS.

Uso de esta política

Puede asociar AmazonElasticTranscoder_JobsSubmitter a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de junio de 2018 a las 21:12 UTC
- Hora de edición: 10 de junio de 2019 a las 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticTranscoder_ReadOnlyAccess

AmazonElasticTranscoder_ReadOnlyAccess es una [política administrada por AWS](#) que: otorga a los usuarios acceso de solo lectura a Elastic Transcoder y acceso a listas de servicios relacionados.

Uso de esta política

Puede asociar AmazonElasticTranscoder_ReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de junio de 2018 a las 21:09 UTC
- Hora de edición: 10 de junio de 2019 a las 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "elastictranscoder:Read*",
      "elastictranscoder:List*",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "iam:ListRoles",
      "sns:ListTopics"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonElasticTranscoderRole

AmazonElasticTranscoderRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio Amazon Elastic Transcoder.

Uso de esta política

Puede asociar AmazonElasticTranscoderRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC

- Hora de edición: 13 de junio de 2019 a las 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEMRCleanupPolicy

AmazonEMRCleanupPolicy es una [política administrada por AWS](#) que: permite las acciones que EMR requiere para terminar y eliminar los recursos EC2 de AWS si el rol de servicio de EMR ha perdido esa capacidad.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de septiembre de 2017 a las 23:54 UTC
- Hora de edición: 29 de septiembre de 2020 a las 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSpotInstanceRequests",
        "ec2>DeleteLaunchTemplate",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:CancelSpotInstanceRequests",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2>DeleteVolume",
        "ec2:DescribePlacementGroups",
        "ec2>DeletePlacementGroup"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEMRContainersServiceRolePolicy

AmazonEMRContainersServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a otros recursos de servicio de AWS necesarios para ejecutar Amazon EMR

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de diciembre de 2020 a las 00:38 UTC
- Hora de edición: 10 de marzo de 2023 a las 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ]
    }
  ]
}
```

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEMRFullAccessPolicy_v2

AmazonEMRFullAccessPolicy_v2 es una [política administrada por AWS](#) que: proporciona acceso completo a Amazon EMR

Uso de esta política

Puede asociar AmazonEMRFullAccessPolicy_v2 a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de marzo de 2021 a la 1:50 UTC
- Hora de edición: 28 de julio de 2023 a las 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
```



```
"Action" : [  
  "elasticmapreduce:AddInstanceFleet",  
  "elasticmapreduce:AddInstanceGroups",  
  "elasticmapreduce:AddJobFlowSteps",  
  "elasticmapreduce:AddTags",  
  "elasticmapreduce:CancelSteps",  
  "elasticmapreduce:CreateEditor",  
  "elasticmapreduce: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" : "*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEMRReadOnlyAccessPolicy_v2

AmazonEMRReadOnlyAccessPolicy_v2 es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon EMR y a las métricas de CloudWatch asociadas.

Uso de esta política

Puede asociar AmazonEMRReadOnlyAccessPolicy_v2 a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de marzo de 2021 a las 1:39 UTC
- Hora de edición: 2 de agosto de 2023 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "elasticmapreduce:DescribeEditor",
    "elasticmapreduce:DescribeJobFlows",
    "elasticmapreduce:DescribeSecurityConfiguration",
    "elasticmapreduce:DescribeStep",
    "elasticmapreduce:DescribeReleaseLabel",
    "elasticmapreduce:GetBlockPublicAccessConfiguration",
    "elasticmapreduce:GetManagedScalingPolicy",
    "elasticmapreduce:GetAutoTerminationPolicy",
    "elasticmapreduce:ListBootstrapActions",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListEditors",
    "elasticmapreduce:ListInstanceFleets",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListInstances",
    "elasticmapreduce:ListSecurityConfigurations",
    "elasticmapreduce:ListSteps",
    "elasticmapreduce:ListSupportedInstanceTypes",
    "elasticmapreduce:ViewEventsFromAllClustersInConsole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ViewMetricsInEMRConsole",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEMRServerlessServiceRolePolicy

AmazonEMRServerlessServiceRolePolicy es una [política administrada de AWS](#) que permite el acceso a otros recursos de servicios de AWS necesarios para ejecutar Amazon EMRServerless

Uso de esta política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de mayo de 2022 a las 23:15 UTC
- Hora editada: 25 de enero de 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchPolicyStatement",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:PutMetricData"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "cloudwatch:namespace" : [
                "AWS/EMRServerless",
                "AWS/Usage"
            ]
        }
    }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEMRServicePolicy_v2

AmazonEMRServicePolicy_v2 es una [política administrada por AWS](#) que: se utiliza para el rol de servicio de Amazon EMR y NO debe utilizarse para ningún otro usuario o rol de IAM en su cuenta. La política otorga permisos para crear y administrar los recursos asociados con EMR y los servicios relacionados necesarios para el funcionamiento del clúster de EMR.

Uso de esta política

Puede asociar AmazonEMRServicePolicy_v2 a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de marzo de 2021 a la 1:11 UTC
- Hora de edición: 15 de febrero de 2022 a las 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
```



```

        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
}
},
{
    "Sid" : "CreateWithEMRTaggedLaunchTemplate",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
},
{
    "Sid" : "CreateEMRTaggedLaunchTemplate",
    "Effect" : "Allow",
    "Action" : "ec2:CreateLaunchTemplate",
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
},
{
    "Sid" : "CreateEMRTaggedInstancesAndVolumes",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
}

```

```

    }
  }
},
{
  "Sid" : "ResourcesToLaunchEC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",
    "ec2:CreateFleet",
    "ec2:CreateLaunchTemplate",
    "ec2:CreateLaunchTemplateVersion"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:image/ami-*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:capacity-reservation/*",
    "arn:aws:ec2:*:*:placement-group/EMR_*",
    "arn:aws:ec2:*:*:fleet/*",
    "arn:aws:ec2:*:*:dedicated-host/*",
    "arn:aws:resource-groups:*:*:group/*"
  ]
},
{
  "Sid" : "ManageEMRTaggedResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplateVersion",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteNetworkInterface",
    "ec2:ModifyInstanceAttribute",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "ManageTagsOnEMRTaggedResources",
  "Effect" : "Allow",
  "Action" : [

```

```

    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "TagOnCreateTaggedEMRResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {

```

```
        "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
        ]
    }
},
{
    "Sid" : "TagPlacementGroups",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags",
        "ec2>DeleteTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
    ]
},
{
    "Sid" : "ListActionsForEC2Resources",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2: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*"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonESCognitoAccess

AmazonESCognitoAccess es una [política administrada por AWS](#) que: proporciona acceso limitado al servicio de configuración de Amazon Cognito.

Uso de esta política

Puede asociar AmazonESCognitoAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de febrero de 2018 a las 22:29 UTC
- Hora de edición: 20 de diciembre de 2021 a las 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```



```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "cognito-idp:DescribeUserPool",
      "cognito-idp:CreateUserPoolClient",
      "cognito-idp>DeleteUserPoolClient",
      "cognito-idp:UpdateUserPoolClient",
      "cognito-idp:DescribeUserPoolClient",
      "cognito-idp:AdminInitiateAuth",
      "cognito-idp:AdminUserGlobalSignOut",
      "cognito-idp:ListUserPoolClients",
      "cognito-identity:DescribeIdentityPool",
      "cognito-identity:UpdateIdentityPool",
      "cognito-identity:SetIdentityPoolRoles",
      "cognito-identity:GetIdentityPoolRoles"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "cognito-identity.amazonaws.com",
          "cognito-identity-us-gov.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonESFullAccess

AmazonESFullAccess es una [política administrada por AWS](#) que: proporciona acceso total al servicio de configuración de Amazon ES.

Uso de esta política

Puede asociar AmazonESFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de octubre de 2015 a las 19:14 UTC
- Hora de edición: 1 de octubre de 2015 a las 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonESReadOnlyAccess

AmazonESReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio de configuración de Amazon ES.

Uso de esta política

Puede asociar AmazonESReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de octubre de 2015 a las 19:18 UTC
- Hora de edición: 3 de octubre de 2018 a las 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

AmazonEventBridgeApiDestinationsServiceRolePolicy es una [política administrada por AWS](#) que: permite a EventBridge acceder a los recursos de Secret Manager en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 11 de febrero de 2021 a las 20:52 UTC
- Hora de edición: 11 de febrero de 2021 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager>DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgeFullAccess

AmazonEventBridgeFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon EventBridge.

Uso de esta política

Puede asociar AmazonEventBridgeFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de julio de 2019 a las 14:08 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    }
  ],
}
```

```

{
  "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
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"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgePipesFullAccess

AmazonEventBridgePipesFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a Amazon EventBridge Pipes.

Uso de esta política

Puede asociar AmazonEventBridgePipesFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2022 a las 17:03 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
```

```
"Action" : "iam:PassRole",
"Resource" : "arn:aws:iam::*:role/*",
"Condition" : {
  "StringLike" : {
    "iam:PassedToService" : "pipes.amazonaws.com"
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgePipesOperatorAccess

AmazonEventBridgePipesOperatorAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura y de operador (posibilidad de detener e iniciar la ejecución de Pipe) a Amazon EventBridge Pipes.

Uso de esta política

Puede asociar AmazonEventBridgePipesOperatorAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2022 a las 17:04 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgePipesReadOnlyAccess

AmazonEventBridgePipesReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon EventBridge Pipes.

Uso de esta política

Puede asociar AmazonEventBridgePipesReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2022 a las 17:04 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgeReadOnlyAccess

AmazonEventBridgeReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon EventBridge.

Uso de esta política

Puede asociar AmazonEventBridgeReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de julio de 2019 a las 13:59 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
```

```
    "scheduler:ListSchedules",
    "scheduler:ListScheduleGroups",
    "scheduler:ListTagsForResource",
    "pipes:DescribePipe",
    "pipes:ListPipes",
    "pipes:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgeSchedulerFullAccess

AmazonEventBridgeSchedulerFullAccess es una [política administrada por AWS](#), AmazonEventBridgeSchedulerFullAccess, que concede permisos para utilizar todas las acciones de EventBridge Scheduler para las programaciones y los grupos de programación.

Uso de esta política

Puede asociar AmazonEventBridgeSchedulerFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de noviembre de 2022 a las 18:37 UTC
- Hora de edición: 10 de noviembre de 2022 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgeSchedulerReadOnlyAccess

AmazonEventBridgeSchedulerReadOnlyAccess es una [política administrada por AWS](#), AmazonEventBridgeSchedulerReadOnlyAccess, que concede permisos de solo lectura para ver los detalles de sus programaciones y grupos de programaciones

Uso de esta política

Puede asociar AmazonEventBridgeSchedulerReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de noviembre de 2022 a las 18:50 UTC
- Hora de edición: 10 de noviembre de 2022 a las 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ]
    }
  ],
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgeSchemasFullAccess

AmazonEventBridgeSchemasFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a los esquemas de Amazon EventBridge.

Uso de esta política

Puede asociar AmazonEventBridgeSchemasFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2019 a las 23:12 UTC
- Hora de edición: 28 de noviembre de 2019 a las 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEventBridgeManageRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam:*:*:role/aws-service-role/schemas.amazonaws.com/AWSServiceRoleForSchemas"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgeSchemasReadOnlyAccess

AmazonEventBridgeSchemasReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a los esquemas de Amazon EventBridge.

Uso de esta política

Puede asociar AmazonEventBridgeSchemasReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2019 a las 23:05 UTC
- Hora de edición: 1 de mayo de 2020 a las 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Action" : [
  "schemas:ListDiscoverers",
  "schemas:DescribeDiscoverer",
  "schemas:ListRegistries",
  "schemas:DescribeRegistry",
  "schemas:SearchSchemas",
  "schemas:ListSchemas",
  "schemas:ListSchemaVersions",
  "schemas:DescribeSchema",
  "schemas:GetDiscoveredSchema",
  "schemas:DescribeCodeBinding",
  "schemas:GetCodeBindingSource",
  "schemas:ListTagsForResource",
  "schemas:GetResourcePolicy"
],
"Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonEventBridgeSchemasServiceRolePolicy

AmazonEventBridgeSchemasServiceRolePolicy es una [política administrada por AWS](#) que otorga permisos a las reglas administradas creadas por los esquemas de Amazon EventBridge.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de noviembre de 2019 a la 1:10 UTC
- Hora de edición: 27 de noviembre de 2019 a la 1:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFISServiceRolePolicy

AmazonFISServiceRolePolicy es una [política administrada por AWS](#) que: permite a FIS AWS administrar la supervisión y la selección de recursos para los experimentos.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de diciembre de 2020 a las 21:18 UTC
- Hora de edición: 25 de octubre de 2022 a las 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "events:PutRule",
  "events>DeleteRule",
  "events:PutTargets",
  "events:RemoveTargets"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "events:ManagedBy" : "fis.amazonaws.com"
  }
}
},
{
  "Sid" : "EventBridgeDescribe",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Tagging",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmHistory"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DescribeUserResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
```



```
    "ec2:DescribeSubnets",
    "iam:GetUser",
    "iam:GetRole",
    "iam:ListUsers",
    "iam:ListRoles",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstances",
    "ecs:DescribeClusters",
    "ecs:DescribeTasks",
    "ecs:ListTasks",
    "eks:DescribeNodegroup",
    "eks:DescribeCluster"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonForecastFullAccess

AmazonForecastFullAccess es una [política administrada por AWS](#) que: brinda acceso a todas las acciones de Amazon Forecast

Uso de esta política

Puede asociar AmazonForecastFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de enero de 2019 a la 1:52 UTC
- Hora de edición: 18 de enero de 2019 a la 1:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFraudDetectorFullAccessPolicy

AmazonFraudDetectorFullAccessPolicy es una [política administrada por AWS](#) que: brinda acceso a todas las acciones de Amazon Fraud Detector

Uso de esta política

Puede asociar AmazonFraudDetectorFullAccessPolicy a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 22:46 UTC
- Hora de edición: 3 de diciembre de 2019 a las 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "frauddetector.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFreeRTOSFullAccess

AmazonFreeRTOSFullAccess es una [política administrada por AWS](#) que: sirve como política de acceso total para Amazon FreeRTOS

Uso de esta política

Puede asociar AmazonFreeRTOSFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2017 a las 15:32 UTC
- Hora de edición: 29 de noviembre de 2017 a las 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFreeRTOSOTAUpdate

AmazonFreeRTOSOTAUpdate es una [política administrada por AWS](#) que: permite al usuario acceder a la actualización transparente de Amazon FreeRTOS

Uso de esta política

Puede asociar AmazonFreeRTOSOTAUpdate a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de agosto de 2018 a las 22:43 UTC
- Hora de edición: 18 de diciembre de 2020 a las 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afri-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" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFSxConsoleFullAccess

AmazonFSxConsoleFullAccess es una [política administrada de AWS](#) que proporciona acceso total a Amazon FSx y acceso a los servicios relacionados AWS a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonFSxConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 28 de noviembre de 2018 a las 16:36 UTC
- Hora editada: 10 de enero de 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFSxConsoleReadOnlyAccess

AmazonFSxConsoleReadOnlyAccess es una [política administrada de AWS](#) que proporciona acceso de solo lectura a Amazon FSx y acceso a los servicios relacionados AWS a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonFSxConsoleReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 28 de noviembre de 2018 a las 16:35 UTC
- Hora editada: 10 de enero de 2024, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFSxFullAccess

AmazonFSxFullAccess es una [política administrada de AWS](#) que proporciona acceso total a Amazon FSx y acceso a los servicios relacionados AWS.

Uso de esta política

Puede asociar AmazonFSxFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 28 de noviembre de 2018 a las 16:34 UTC
- Hora editada: 10 de enero de 2024, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

```
        "iam.amazonaws.com"
      ]
    }
  }
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFSxReadOnlyAccess

AmazonFSxReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon FSx.

Uso de esta política

Puede asociar AmazonFSxReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2018 a las 16:33 UTC
- Hora de edición: 28 de noviembre de 2018 a las 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonFSxServiceRolePolicy

AmazonFSxServiceRolePolicy es una [política administrada de AWS](#) que permite a Amazon FSx administrar los recursos AWS en su nombre

Uso de esta política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 28 de noviembre de 2018 a las 10:38 UTC
- Hora editada: 10 de enero de 2024, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PutMetrics",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/FSx"
      }
    }
  },
  {
    "Sid" : "TagResourceNetworkInterface",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "AmazonFSx.FileSystemId"
      }
    }
  },
  {
    "Sid" : "ManageNetworkInterface",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssignPrivateIpAddresses",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:UnassignPrivateIpAddresses"
    ],
  },
```

```
"Resource" : [
  "arn:aws:ec2:*:*:network-interface/*"
],
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
  }
}
},
{
  "Sid" : "ManageRouteTable",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateRoute",
    "ec2:ReplaceRoute",
    "ec2>DeleteRoute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
    }
  }
},
{
  "Sid" : "PutCloudWatchLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
},
{
  "Sid" : "ManageAuditLogs",
  "Effect" : "Allow",
  "Action" : [
    "firehose:DescribeDeliveryStream",
    "firehose:PutRecord",
    "firehose:PutRecordBatch"
  ]
},
```

```
    "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
  }
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGlacierFullAccess

AmazonGlacierFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Glacier a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonGlacierFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```



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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGlacierReadOnlyAccess

AmazonGlacierReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Glacier a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonGlacierReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 5 de mayo de 2016 a las 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListMultipartUploads",
        "glacier:ListParts",
        "glacier:ListTagsForVault",
        "glacier:ListVaults"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGrafanaAthenaAccess

AmazonGrafanaAthenaAccess es una [política administrada por AWS](#) que: otorga acceso a Amazon Athena y a las dependencias necesarias para poder consultar y escribir los resultados en s3 desde el complemento Amazon Athena de Amazon Grafana.

Uso de esta política

Puede asociar AmazonGrafanaAthenaAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de noviembre de 2021 a las 17:11 UTC
- Hora de edición: 22 de noviembre de 2021 a las 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
```

```

    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListTableMetadata",
    "athena:ListWorkGroups"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetWorkGroup",
    "athena:StartQueryExecution",
    "athena:StopQueryExecution"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/GrafanaDataSource" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchGetPartition"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",

```

```
"Action" : [
  "s3:GetBucketLocation",
  "s3:GetObject",
  "s3:ListBucket",
  "s3:ListBucketMultipartUploads",
  "s3:ListMultipartUploadParts",
  "s3:AbortMultipartUpload",
  "s3:CreateBucket",
  "s3:PutObject",
  "s3:PutBucketPublicAccessBlock"
],
"Resource" : [
  "arn:aws:s3:::grafana-athena-query-results-*"
]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGrafanaCloudWatchAccess

AmazonGrafanaCloudWatchAccess es una [política administrada por AWS](#) que: otorga acceso a Amazon CloudWatch y a las dependencias necesarias para utilizar CloudWatch como fuente de datos en Amazon Managed Grafana.

Uso de esta política

Puede asociar AmazonGrafanaCloudWatchAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de marzo de 2023 a las 22:41 UTC
- Hora de edición: 24 de marzo de 2023 a las 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetInsightRuleReport"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:GetLogGroupFields",
        "logs:StartQuery",
        "logs:StopQuery",

```

```
    "logs:GetQueryResults",
    "logs:GetLogEvents"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeRegions"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "tag:GetResources",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "oam:ListSinks",
    "oam:ListAttachedLinks"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGrafanaRedshiftAccess

AmazonGrafanaRedshiftAccess es una [política administrada por AWS](#) que: otorga acceso limitado a Amazon Redshift y a las dependencias necesarias para utilizar el complemento Amazon Redshift en Amazon Grafana.

Uso de esta política

Puede asociar AmazonGrafanaRedshiftAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de noviembre de 2021 a las 23:15 UTC
- Hora de edición: 26 de noviembre de 2021 a las 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    }
  ]
}
```



```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    }
  ],
  {
    "Effect" : "Allow",
    "Action" : "redshift:GetClusterCredentials",
    "Resource" : [
      "arn:aws:redshift:*:*:dbname:*/*",
      "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGrafanaServiceLinkedRolePolicy

AmazonGrafanaServiceLinkedRolePolicy es una [política administrada por AWS](#) que: proporciona acceso a los recursos AWS gestionados o utilizados por Amazon Grafana.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de noviembre de 2022 a las 23:10 UTC
- Hora de edición: 8 de noviembre de 2022 a las 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "AmazonGrafanaManaged"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "Null" : {
        "aws:RequestTag/AmazonGrafanaManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2>DeleteNetworkInterface",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
      }
    }
  }
}

```

```
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGuardDutyFullAccess

AmazonGuardDutyFullAccesses una [política AWS gestionada](#) que: proporciona acceso total para usar Amazon GuardDuty.

Uso de la política

Puede asociar AmazonGuardDutyFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 28 de noviembre de 2017 a las 22:31 UTC
- Hora editada: 16 de noviembre de 2023 a las 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

"Statement" : [
  {
    "Sid" : "AmazonGuardDutyFullAccessSid1",
    "Effect" : "Allow",
    "Action" : "guardduty:*",
    "Resource" : "*"
  },
  {
    "Sid" : "CreateServiceLinkedRoleSid1",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [
          "guardduty.amazonaws.com",
          "malware-protection.guardduty.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ActionsForOrganizationsSid1",
    "Effect" : "Allow",
    "Action" : [
      "organizations:EnableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IamGetRoleSid1",
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
  }
]

```

}

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

AmazonGuardDutyMalwareProtectionServiceRolePolicy es una [política AWS gestionada](#) que: la protección contra GuardDuty malware utiliza el rol vinculado al servicio (SLR) denominado. AWSServiceRoleForAmazonGuardDutyMalwareProtection Esta función vinculada al servicio permite a la protección contra GuardDuty malware realizar escaneos sin agentes para detectar malware. Permite GuardDuty crear instantáneas en su cuenta y compartirlas con la cuenta de GuardDuty servicio para detectar malware. Evalúa estas instantáneas compartidas e incluye los metadatos de la instancia EC2 recuperados en las conclusiones sobre la protección contra el malware. GuardDuty La función AWSServiceRoleForAmazonGuardDutyMalwareProtection vinculada al servicio confía en que el servicio malware-protection.guardduty.amazonaws.com la asumirá.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de julio de 2022 a las 19:06 UTC
- Hora editada: 25 de enero de 2024 a las 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
```

```
"Resource" : "arn:aws:ec2:*:*:snapshot/*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:TagKeys" : "GuardDutyScanId"
  }
},
{
  "Sid" : "CreateTagsPermission",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:*/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateSnapshot"
    }
  }
},
{
  "Sid" : "AddTagsToSnapshotPermission",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/GuardDutyScanId" : "*"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "GuardDutyExcluded",
        "GuardDutyFindingDetected"
      ]
    }
  }
},
{
  "Sid" : "DeleteAndShareSnapshotPermission",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSnapshot",
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
```



```

    "StringLike" : {
      "ec2:ResourceTag/GuardDutyScanId" : "*"
    },
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    }
  }
},
{
  "Sid" : "PreventPublicAccessToSnapshotPermission",
  "Effect" : "Deny",
  "Action" : [
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:Add/group" : "all"
    }
  }
},
{
  "Sid" : "CreateGrantPermission",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    },
    "StringLike" : {
      "kms:EncryptionContext:aws:ebs:id" : "snap-*"
    },
    "ForAllValues:StringEquals" : {
      "kms:GrantOperations" : [
        "Decrypt",
        "CreateGrant",
        "GenerateDataKeyWithoutPlaintext",
        "ReEncryptFrom",
        "ReEncryptTo",
        "RetireGrant",
        "DescribeKey"
      ]
    }
  }
},

```

```
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    }
  },
  {
    "Sid" : "ShareSnapshotKMSPermission",
    "Effect" : "Allow",
    "Action" : [
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
    ],
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "ec2.*.amazonaws.com"
      },
      "Null" : {
        "aws:ResourceTag/GuardDutyExcluded" : "true"
      }
    }
  },
  {
    "Sid" : "DescribeKeyPermission",
    "Effect" : "Allow",
    "Action" : "kms:DescribeKey",
    "Resource" : "arn:aws:kms:*:*:key/*"
  },
  {
    "Sid" : "GuardDutyLogGroupPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups",
      "logs:CreateLogGroup",
      "logs:PutRetentionPolicy"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
  },
  {
    "Sid" : "GuardDutyLogStreamPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
```

```
    "logs:DescribeLogStreams"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
},
{
  "Sid" : "EBSDirectAPIPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ebs:GetSnapshotBlock",
    "ebs:ListSnapshotBlocks"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/GuardDutyScanId" : "*"
    },
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    }
  }
}
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGuardDutyReadOnlyAccess

AmazonGuardDutyReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a GuardDuty los recursos de Amazon

Uso de la política

Puede asociar AmazonGuardDutyReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada de AWS
- Hora de creación: 28 de noviembre de 2017 a las 22:29 UTC
- Hora editada: 16 de noviembre de 2023 a las 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonGuardDutyServiceRolePolicy

AmazonGuardDutyServiceRolePolicy es una [política AWS gestionada](#) que: permite el acceso a AWS los recursos utilizados o gestionados por Amazon Guard Duty

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 28 de noviembre de 2017 a las 20:12 UTC
- Hora editada: 9 de febrero de 2024 a las 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2: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"
      ]
    }
  }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonHealthLakeFullAccess

AmazonHealthLakeFullAccess es una [política administrada por AWS](#) que: proporciona acceso total al servicio Amazon HealthLake.

Uso de esta política

Puede asociar `AmazonHealthLakeFullAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de febrero de 2021 a la 1:07 UTC
- Hora de edición: 17 de febrero de 2021 a la 1:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
```

```
    "StringEquals" : {
      "iam:PassedToService" : "healthlake.amazonaws.com"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonHealthLakeReadOnlyAccess

AmazonHealthLakeReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio Amazon HealthLake.

Uso de esta política

Puede asociar AmazonHealthLakeReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de febrero de 2021 a las 2:43 UTC
- Hora de edición: 17 de febrero de 2021 a las 2:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonHoneycodeFullAccess

AmazonHoneycodeFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Honeycode a través de AWS Management Console y SDK.

Uso de esta política

Puede asociar `AmazonHoneycodeFullAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 24 de junio de 2020 a las 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonHoneycodeReadOnlyAccess

AmazonHoneycodeReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Honeycode a través de AWS Management Console y SDK.

Uso de esta política

Puede asociar AmazonHoneycodeReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "honeycode:List*",
        "honeycode:Get*",
        "honeycode:Describe*",
        "honeycode:Query*"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonHoneycodeServiceRolePolicy

AmazonHoneycodeServiceRolePolicy es una [política administrada por AWS](#) que: tiene un rol vinculado a un servicio necesario para que Amazon Honeycode acceda a sus recursos.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2020 a las 18:03 UTC
- Hora de edición: 18 de noviembre de 2020 a las 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonHoneycodeTeamAssociationFullAccess

AmazonHoneycodeTeamAssociationFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Honeycode Team Association a través de AWS Management Console y SDK.

Uso de esta política

Puede asociar AmazonHoneycodeTeamAssociationFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 24 de junio de 2020 a las 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

AmazonHoneycodeTeamAssociationReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Honeycode Team Association a través de AWS Management Console y SDK.

Uso de esta política

Puede asociar AmazonHoneycodeTeamAssociationReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2020 a las 20:27 UTC
- Hora de edición: 24 de junio de 2020 a las 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations"
      ]
    }
  ]
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonHoneycodeWorkbookFullAccess

AmazonHoneycodeWorkbookFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a Honeycode Workbook a través de AWS Management Console y SDK.

Uso de esta política

Puede asociar AmazonHoneycodeWorkbookFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode>ListTableColumns",
        "honeycode>ListTableRows",
        "honeycode>ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonHoneycodeWorkbookReadOnlyAccess

AmazonHoneycodeWorkbookReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Honeycode Workbook a través de AWS Management Console y SDK.

Uso de esta política

Puede asociar AmazonHoneycodeWorkbookReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ]
    }
  ],
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonInspector2AgentlessServiceRolePolicy

AmazonInspector2AgentlessServiceRolePolicy es una [política AWS gestionada](#) que: otorga a Amazon Inspector acceso a las evaluaciones de Servicios de AWS seguridad necesarias para realizar las evaluaciones de seguridad sin agentes

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de noviembre de 2023 a las 15:18 UTC
- Hora editada: 20 de noviembre de 2023 a las 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume*"
      ]
    }
  ],
  {
```



```

    "Sid" : "DenyCreateSnapshotsOnExcludedInstances",
    "Effect" : "Deny",
    "Action" : "ec2:CreateSnapshots",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
      }
    }
  },
  {
    "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSnapshots",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:TagKeys" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "InspectorScan"
      }
    }
  },
  {
    "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:CreateAction" : "CreateSnapshots"
      },
      "Null" : {
        "aws:TagKeys" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "InspectorScan"
      }
    }
  },
  {
    "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
    "Effect" : "Allow",

```

```

    "Action" : "ec2:DeleteSnapshot",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/InspectorScan" : "*"
      }
    }
  },
  {
    "Sid" : "DenyKmsDecryptForExcludedKeys",
    "Effect" : "Deny",
    "Action" : "kms:Decrypt",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/InspectorEc2Exclusion" : "true"
      }
    }
  },
  {
    "Sid" : "DecryptSnapshotBlocksVolContext",
    "Effect" : "Allow",
    "Action" : "kms:Decrypt",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      },
      "StringLike" : {
        "kms:ViaService" : "ec2.*.amazonaws.com",
        "kms:EncryptionContext:aws:ebs:id" : "vol-*"
      }
    }
  },
  {
    "Sid" : "DecryptSnapshotBlocksSnapContext",
    "Effect" : "Allow",
    "Action" : "kms:Decrypt",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      },
      "StringLike" : {

```

```
        "kms:ViaService" : "ec2.*.amazonaws.com",
        "kms:EncryptionContext:aws:ebs:id" : "snap-*"
    }
}
},
{
    "Sid" : "DescribeKeysForEbsOperations",
    "Effect" : "Allow",
    "Action" : "kms:DescribeKey",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
            "kms:ViaService" : "ec2.*.amazonaws.com"
        }
    }
},
{
    "Sid" : "ListKeyResourceTags",
    "Effect" : "Allow",
    "Action" : "kms:ListResourceTags",
    "Resource" : "arn:aws:kms:*:*:key/*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonInspector2FullAccess

AmazonInspector2FullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Inspector y acceso a otros servicios relacionados, como las organizaciones.

Uso de esta política

Puede asociar `AmazonInspector2FullAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2021 a las 19:10 UTC
- Hora de edición: 3 de agosto de 2023 a las 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonInspector2ManagedCisPolicy

AmazonInspector2ManagedCisPolicy es una [política AWS gestionada](#) que: se trata de una política gestionada que el cliente debe adjuntar a sus funciones para comunicarse con el servicio de inspección para los escaneos del CIS

Uso de la política

Puede asociar `AmazonInspector2ManagedCisPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de enero de 2024 a las 16:31 UTC
- Hora editada: 24 de enero de 2024 a las 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonInspector2ReadOnlyAccess

AmazonInspector2ReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio Amazon inspector2 y a los servicios de soporte pertinentes

Uso de esta política

Puede asociar AmazonInspector2ReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de enero de 2022 a las 14:45 UTC
- Hora de edición: 22 de septiembre de 2023 a las 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "inspector2:BatchGet*",
      "inspector2:List*",
      "inspector2:Describe*",
      "inspector2:Get*",
      "inspector2:Search*",
      "codeguru-security:BatchGetFindings",
      "codeguru-security:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonInspector2ServiceRolePolicy

AmazonInspector2ServiceRolePolicy es una [política administrada por AWS](#) que: otorga a Amazon Inspector acceso a Servicios de AWS necesario para realizar las evaluaciones de seguridad

Uso de esta política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de noviembre de 2021 a las 20:27 UTC
- Hora editada: 22 de enero de 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Versión de la política

Versión de la política: v12 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonInspectorFullAccess

AmazonInspectorFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Inspector.

Uso de esta política

Puede asociar AmazonInspectorFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de octubre de 2015 a las 17:08 UTC
- Hora de edición: 21 de diciembre de 2017 a las 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ]
    }
  ]
}
```



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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonInspectorReadOnlyAccess

AmazonInspectorReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Inspector.

Uso de esta política

Puede asociar AmazonInspectorReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de octubre de 2015 a las 17:08 UTC
- Hora de edición: 1 de octubre de 2019 a las 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonInspectorServiceRolePolicy

AmazonInspectorServiceRolePolicy es una [política administrada por AWS](#) que: otorga a Amazon Inspector acceso a Servicios de AWS necesario para realizar las evaluaciones de seguridad

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de noviembre de 2017 a las 15:48 UTC
- Hora de edición: 11 de septiembre de 2020 a las 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "directconnect:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayVpcAttachments",

```

```
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:SearchTransitGatewayRoutes",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKendraFullAccess

AmazonKendraFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Kendra a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonKendraFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 16:15 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kendra.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
```

```
    "kms:ListAliases",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:DescribeSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
},
{
  "Effect" : "Allow",
  "Action" : "kendra:*",
  "Resource" : "*"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKendraReadOnlyAccess

AmazonKendraReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Kendra a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonKendraReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 16:13 UTC
- Hora de edición: 27 de mayo de 2021 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "kendra:Describe*",
      "kendra:List*",
      "kendra:Query",
      "kendra:GetQuerySuggestions"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKeyspacesFullAccess

AmazonKeyspacesFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a Amazon Keyspaces

Uso de esta política

Puede asociar AmazonKeyspacesFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de abril de 2020 a las 17:06 UTC
- Hora de edición: 3 de octubre de 2023 a las 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
```

```

    "Action" : [
      "cloudwatch:DeleteAlarms",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:GetMetricData",
      "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ApplicationAutoscalingServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "KeyspacesReplicationServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "Ec2VpcReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeVpcEndpoints"
    ],
    "Resource" : "*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKeyspacesReadOnlyAccess

AmazonKeyspacesReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Keyspaces

Uso de esta política

Puede asociar AmazonKeyspacesReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de abril de 2020 a las 17:07 UTC
- Hora de edición: 7 de julio de 2022 a las 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "cassandra:Select"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingActivities",
      "application-autoscaling:DescribeScalingPolicies",
      "application-autoscaling:DescribeScheduledActions",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:GetMetricData",
      "kms:DescribeKey",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKeyspacesReadOnlyAccess_v2

AmazonKeyspacesReadOnlyAccess_v2 es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Keyspaces y servicios relacionados AWS.

Uso de esta política

Puede asociar `AmazonKeyspacesReadOnlyAccess_v2` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de septiembre de 2023 a las 17:01 UTC
- Hora de edición: 12 de septiembre de 2023 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
```

```
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKinesisAnalyticsFullAccess

AmazonKinesisAnalyticsFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Kinesis Analytics a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonKinesisAnalyticsFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de septiembre de 2016 a las 19:01 UTC
- Hora de edición: 21 de septiembre de 2016 a las 19:01 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisanalytics:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis>DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```



```
    "Action" : [
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "logs:GetLogEvents",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListPolicyVersions",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/kinesis-analytics*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKinesisAnalyticsReadOnly

AmazonKinesisAnalyticsReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Kinesis Analytics a través de AWS Management Console.

Uso de esta política

Puede asociar `AmazonKinesisAnalyticsReadOnly` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de septiembre de 2016 a las 18:16 UTC
- Hora de edición: 21 de septiembre de 2016 a las 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:DescribeDeliveryStream",
      "firehose:ListDeliveryStreams"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "logs:GetLogEvents",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListPolicyVersions",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKinesisFirehoseFullAccess

AmazonKinesisFirehoseFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todos los flujos de entrega de Amazon Kinesis Firehose.

Uso de esta política

Puede asociar AmazonKinesisFirehoseFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de octubre de 2015 a las 18:45 UTC
- Hora de edición: 7 de octubre de 2015 a las 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKinesisFirehoseReadOnlyAccess

AmazonKinesisFirehoseReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a todos los flujos de entrega de Amazon Kinesis Firehose.

Uso de esta política

Puede asociar AmazonKinesisFirehoseReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de octubre de 2015 a las 18:43 UTC
- Hora de edición: 7 de octubre de 2015 a las 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKinesisFullAccess

AmazonKinesisFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todos los flujos a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonKinesisFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKinesisReadOnlyAccess

AmazonKinesisReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a todas las transmisiones a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonKinesisReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKinesisVideoStreamsFullAccess

AmazonKinesisVideoStreamsFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Kinesis Video Streams a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonKinesisVideoStreamsFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2017 a las 23:27 UTC
- Hora de edición: 1 de diciembre de 2017 a las 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonKinesisVideoStreamsReadOnlyAccess

AmazonKinesisVideoStreamsReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a AWS Kinesis Video Streams a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonKinesisVideoStreamsReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2017 a las 23:14 UTC
- Hora de edición: 1 de diciembre de 2017 a las 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLaunchWizard_Fullaccess

AmazonLaunchWizard_Fullaccess es una [política administrada por AWS](#) que ofrece acceso total al asistente de lanzamiento de AWS y a otros servicios necesarios.

Uso de esta política

Puede asociar AmazonLaunchWizard_Fullaccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 6 de agosto de 2020 a las 17:47 UTC
- Hora de edición: 22 de febrero de 2023 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Versión de la política

Versión de la política: v15 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketLocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:List*",
    "cloudwatch:Get*",
    "cloudwatch:Describe*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateVpc",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AllocateHosts",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssociateAddress",
    "ec2:CreateDhcpOptions",
```

```
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateNetworkInterface",
"ec2:CreateVolume",
"ec2:CreateVpcEndpoint",
"ec2:CreateTags",
"ec2>DeleteTags",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:ModifyInstanceAttribute",
"ec2:ModifySubnetAttribute",
"ec2:ModifyVolumeAttribute",
"ec2:ModifyVpcAttribute",
"ec2:AssociateDhcpOptions",
"ec2:AssociateSubnetCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AttachVolume",
"ec2>DeleteDhcpOptions",
"ec2>DeleteInternetGateway",
"ec2>DeleteKeyPair",
"ec2>DeleteNatGateway",
"ec2>DeleteSecurityGroup",
"ec2>DeleteVolume",
"ec2>DeleteVpc",
"ec2:DetachInternetGateway",
"ec2:DetachVolume",
"ec2>DeleteSnapshot",
"ec2:AssociateRouteTable",
"ec2:AssociateVpcCidrBlock",
"ec2>DeleteNetworkAcl",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2>DeleteRoute",
"ec2>DeleteRouteTable",
"ec2>DeleteSubnet",
"ec2:DetachNetworkInterface",
"ec2:DisassociateAddress",
"ec2:DisassociateVpcCidrBlock",
"ec2:GetLaunchTemplateData",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifyVolume",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:GetConsoleOutput",
"ec2:GetPasswordData",
```

```

    "ec2:ReleaseAddress",
    "ec2:ReplaceRoute",
    "ec2:ReplaceRouteTableAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:DisassociateIamInstanceProfile",
    "ec2:DisassociateRouteTable",
    "ec2:DisassociateSubnetCidrBlock",
    "ec2:ModifyInstancePlacement",
    "ec2>DeletePlacementGroup",
    "ec2>CreatePlacementGroup",
    "elasticfilesystem>DeleteFileSystem",
    "elasticfilesystem>DeleteMountTarget",
    "ds:AddIpRoutes",
    "ds:CreateComputer",
    "ds:CreateMicrosoftAD",
    "ds>DeleteDirectory",
    "servicecatalog:AssociateProductWithPortfolio",
    "cloudformation:GetTemplateSummary",
    "sts:GetCallerIdentity"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStack*",
    "cloudformation:Get*",
    "cloudformation:ListStacks",
    "cloudformation:SignalResource",
    "cloudformation>DeleteStack"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/LaunchWizard*/**",
    "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/**"
  ]
},
{
  "Effect" : "Allow",

```

```

    "Action" : [
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam:AddRoleToInstanceProfile"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
      "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
      "arn:aws:iam:*:*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
      "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ],
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : [
          "lambda.amazonaws.com",
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn"
        ]
      }
    }
  }
}

```



```

},
{
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling>CreateOrUpdateTags",
    "logs:CreateLogStream",
    "logs>DeleteLogGroup",
    "logs>DeleteLogStream",
    "logs:DescribeLog*",
    "logs:PutLogEvents",
    "resource-groups:CreateGroup",
    "resource-groups>DeleteGroup",
    "sns:ListSubscriptionsByTopic",
    "sns:Publish",
    "ssm>DeleteDocument",
    "ssm>DeleteParameter*",
    "ssm:DescribeDocument*",
    "ssm:GetDocument",
    "ssm:PutParameter"
  ],
  "Resource" : [
    "arn:aws:resource-groups:*:*:group/LaunchWizard*",
    "arn:aws:sns:*:*:*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
    "arn:aws:ssm:*:*:parameter/LaunchWizard*",
    "arn:aws:ssm:*:*:document/LaunchWizard*",
    "arn:aws:logs:*:*:log-group:*:*:*",
    "arn:aws:logs:*:*:log-group:LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetDocument",
    "ssm:SendCommand"
  ]
}

```

```

    ],
    "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunShellScript"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:SendCommand"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "logs:DeleteLogStream",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",

```

```

    "cloudformation:DescribeStackDriftDetectionStatus",
    "cloudformation:List*",
    "cloudformation:ValidateTemplate",
    "ds:Describe*",
    "ds:ListAuthorizedApplications",
    "ec2:Describe*",
    "ec2:Get*",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:List*",
    "logs:CreateLogGroup",
    "logs:GetLogDelivery",
    "logs:GetLogRecord",
    "logs:ListLogDeliveries",
    "resource-groups:Get*",
    "resource-groups:List*",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListServiceQuotas",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "ssm:CreateDocument",
    "ssm:DescribeAutomation*",
    "ssm:DescribeInstanceInformation",
    "ssm:DescribeParameters",
    "ssm:GetAutomationExecution",
    "ssm:GetCommandInvocation",
    "ssm:GetParameter*",
    "ssm:GetConnectionStatus",
    "ssm:ListCommand*",
    "ssm:ListDocument*",
    "ssm:ListInstanceAssociations",
    "ssm:SendAutomationSignal",
    "tag:Get*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution",
    "ssm:StopAutomationExecution"
  ]
}

```

```

    ],
    "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "logs:GetLog*",
    "Resource" : [
      "arn:aws:logs:*:*:log-group:*:*:*",
      "arn:aws:logs:*:*:log-group:LaunchWizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:List*",
      "cloudformation:Describe*"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "autoscaling.amazonaws.com",
          "application-insights.amazonaws.com",
          "events.amazonaws.com",
          "autoscaling.amazonaws.com.cn",
          "events.amazonaws.com.cn"
        ]
      }
    }
  }
},
{
  "Effect" : "Allow",

```

```

    "Action" : "launchwizard:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:TagQueue",
      "sqs:GetQueueUrl",
      "sqs:AddPermission",
      "sqs:ListQueues",
      "sqs>DeleteQueue",
      "sqs:GetQueueAttributes",
      "sqs:ListQueueTags",
      "sqs:CreateQueue",
      "sqs:SetQueueAttributes"
    ],
    "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "iam:GetInstanceProfile",
      "cloudwatch>DeleteAlarms",
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : [
      "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
      "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "route53:ListHostedZones",
      "ec2:CreateSecurityGroup",
      "ec2:AuthorizeSecurityGroupIngress",
      "elasticfilesystem:DescribeFileSystems",
      "elasticfilesystem:CreateFileSystem",
      "elasticfilesystem:CreateMountTarget",
      "elasticfilesystem:DescribeMountTargets",
      "elasticfilesystem:DescribeMountTargetSecurityGroups"
    ],
  },

```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::launchwizard*",
      "arn:aws:s3:::launchwizard*/**",
      "arn:aws:s3:::aws-sap-data-provider/config.properties"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudformation:TagResource",
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : "LaunchWizard*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:PutBucketVersioning",
      "s3>DeleteBucket",
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:GetFunction",
      "lambda:GetFunctionConfiguration",
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:LaunchWizard*",
      "arn:aws:s3:::launchwizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
```

```

    "dynamodb:CreateTable",
    "dynamodb:DescribeTable",
    "dynamodb>DeleteTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource",
    "secretsmanager:UntagResource",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager>DeleteResourcePolicy",
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateOpsMetadata"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm>DeleteOpsMetadata",
  "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",

```

```

    "sns:DeleteTopic",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:UntagResource",
    "fsx:TagResource",
    "fsx>DeleteFileSystem",
    "fsx:ListTagsForResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/Name" : "LaunchWizard*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx>CreateFileSystem"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/Name" : [
        "LaunchWizard*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeFileSystems"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",

```



```

"Action" : [
  "servicecatalog:CreatePortfolio",
  "servicecatalog:DescribePortfolio",
  "servicecatalog:CreateConstraint",
  "servicecatalog:CreateProduct",
  "servicecatalog:AssociatePrincipalWithPortfolio",
  "servicecatalog:CreateProvisioningArtifact",
  "servicecatalog:TagResource",
  "servicecatalog:UntagResource"
],
"Resource" : [
  "arn:aws:servicecatalog:*:*:*/*",
  "arn:aws:catalog:*:*:*/*"
],
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : "launchwizard.amazonaws.com"
  }
}
},
{
  "Sid" : "VisualEditor0",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm>DeleteAssociation"
  ],
  "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:UntagResource",
    "elasticfilesystem:TagResource"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
}

```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:TagResource",
    "logs:UntagResource"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLaunchWizardFullAccessV2

AmazonLaunchWizardFullAccessV2 es una [política administrada por AWS](#) que ofrece acceso total al asistente de lanzamiento de AWS y a otros servicios necesarios.

Uso de esta política

Puede asociar AmazonLaunchWizardFullAccessV2 a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 1 de septiembre de 2023 a las 17:14 UTC
- Hora de edición: 1 de septiembre de 2023 a las 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Sid" : "Route53Actions0",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
{
  "Sid" : "S3Actions0",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketLocation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsActions0",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchActions0",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:List*",
    "cloudwatch:Get*",
    "cloudwatch:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2Actions0",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateVpc",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet"
  ],
  "Resource" : "*"
},
{
```

```
"Sid" : "Ec2Actions1",
"Effect" : "Allow",
"Action" : [
  "ec2:AllocateAddress",
  "ec2:AllocateHosts",
  "ec2:AssignPrivateIpAddresses",
  "ec2:AssociateAddress",
  "ec2:CreateDhcpOptions",
  "ec2:CreateEgressOnlyInternetGateway",
  "ec2:CreateNetworkInterface",
  "ec2:CreateVolume",
  "ec2:CreateVpcEndpoint",
  "ec2:CreateTags",
  "ec2>DeleteTags",
  "ec2:RunInstances",
  "ec2:StartInstances",
  "ec2:ModifyInstanceAttribute",
  "ec2:ModifySubnetAttribute",
  "ec2:ModifyVolumeAttribute",
  "ec2:ModifyVpcAttribute",
  "ec2:AssociateDhcpOptions",
  "ec2:AssociateSubnetCidrBlock",
  "ec2:AttachInternetGateway",
  "ec2:AttachNetworkInterface",
  "ec2:AttachVolume",
  "ec2>DeleteDhcpOptions",
  "ec2>DeleteInternetGateway",
  "ec2>DeleteKeyPair",
  "ec2>DeleteNatGateway",
  "ec2>DeleteSecurityGroup",
  "ec2>DeleteVolume",
  "ec2>DeleteVpc",
  "ec2:DetachInternetGateway",
  "ec2:DetachVolume",
  "ec2>DeleteSnapshot",
  "ec2:AssociateRouteTable",
  "ec2:AssociateVpcCidrBlock",
  "ec2>DeleteNetworkAcl",
  "ec2>DeleteNetworkInterface",
  "ec2>DeleteNetworkInterfacePermission",
  "ec2>DeleteRoute",
  "ec2>DeleteRouteTable",
  "ec2>DeleteSubnet",
  "ec2:DetachNetworkInterface",
```

```

    "ec2:DisassociateAddress",
    "ec2:DisassociateVpcCidrBlock",
    "ec2:GetLaunchTemplateData",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifyVolume",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:GetConsoleOutput",
    "ec2:GetPasswordData",
    "ec2:ReleaseAddress",
    "ec2:ReplaceRoute",
    "ec2:ReplaceRouteTableAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:DisassociateIamInstanceProfile",
    "ec2:DisassociateRouteTable",
    "ec2:DisassociateSubnetCidrBlock",
    "ec2:ModifyInstancePlacement",
    "ec2>DeletePlacementGroup",
    "ec2>CreatePlacementGroup",
    "elasticfilesystem:DeleteFileSystem",
    "elasticfilesystem:DeleteMountTarget",
    "ds:AddIpRoutes",
    "ds:CreateComputer",
    "ds:CreateMicrosoftAD",
    "ds>DeleteDirectory",
    "servicecatalog:AssociateProductWithPortfolio",
    "cloudformation:GetTemplateSummary",
    "sts:GetCallerIdentity"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudFormationActions0",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStack*",
    "cloudformation:Get*",
    "cloudformation:ListStacks",
    "cloudformation:SignalResource",

```

```

    "cloudformation:DeleteStack"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/LaunchWizard*/**",
    "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/**"
  ]
},
{
  "Sid" : "Ec2Actions2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/**"
    }
  }
},
{
  "Sid" : "IamActions0",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam:AddRoleToInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
    "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
  ]
},
{
  "Sid" : "IamActions1",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard",

```

```

    "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard",
    "arn:aws:iam::*:instance-profile/LaunchWizard*"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Sid" : "AutoScalingActions0",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:CreateOrUpdateTags",
    "resource-groups:CreateGroup",
    "resource-groups>DeleteGroup",
    "sns:ListSubscriptionsByTopic",
    "sns:Publish",
    "ssm>DeleteDocument",
    "ssm>DeleteParameter*",
    "ssm:DescribeDocument*",
    "ssm:GetDocument",
    "ssm:PutParameter"
  ],
  "Resource" : [
    "arn:aws:resource-groups::*:group/LaunchWizard*",
    "arn:aws:sns::*:*",
    "arn:aws:autoscaling::*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
    "arn:aws:autoscaling::*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
    "arn:aws:ssm::*:parameter/LaunchWizard*",
    "arn:aws:ssm::*:document/LaunchWizard*"
  ]
}

```



```

    },
    {
      "Sid" : "SsmActions0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Sid" : "SsmActions1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*::instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
            "arn:aws:cloudformation:*::stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "SsmActions2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*::parameter/LaunchWizard*",
        "arn:aws:ssm:*::document/LaunchWizard*"
      ]
    },
  ],
  {

```

```

    "Sid" : "SsmActions3",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:Describe*",
      "cloudformation:DescribeAccountLimits",
      "cloudformation:DescribeStackDriftDetectionStatus",
      "cloudformation:List*",
      "cloudformation:ValidateTemplate",
      "ds:Describe*",
      "ds:ListAuthorizedApplications",
      "ec2:Describe*",
      "ec2:Get*",
      "iam:GetRole",
      "iam:GetRolePolicy",
      "iam:GetUser",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:List*",
      "resource-groups:Get*",
      "resource-groups:List*",
      "servicequotas:GetServiceQuota",
      "servicequotas:ListServiceQuotas",
      "sns:ListSubscriptions",
      "sns:ListTopics",
      "ssm:CreateDocument",
      "ssm:DescribeAutomation*",
      "ssm:DescribeInstanceInformation",
      "ssm:DescribeParameters",
      "ssm:GetAutomationExecution",
      "ssm:GetCommandInvocation",
      "ssm:GetParameter*",
      "ssm:GetConnectionStatus",
      "ssm:ListCommand*",
      "ssm:ListDocument*",
      "ssm:ListInstanceAssociations",
      "ssm:SendAutomationSignal",
      "tag:Get*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SsmActions4",
    "Effect" : "Allow",
    "Action" : [

```

```

    "ssm:StartAutomationExecution",
    "ssm:StopAutomationExecution"
  ],
  "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudFormationActions1",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:List*",
    "cloudformation:Describe*"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
},
{
  "Sid" : "IamActions2",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "autoscaling.amazonaws.com",
        "application-insights.amazonaws.com",
        "events.amazonaws.com",
        "autoscaling.amazonaws.com.cn",
        "events.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Sid" : "LaunchWizardActions0",
  "Effect" : "Allow",
  "Action" : "launchwizard:*",
  "Resource" : "*"
},

```

```

{
  "Sid" : "SqsActions0",
  "Effect" : "Allow",
  "Action" : [
    "sqs:TagQueue",
    "sqs:GetQueueUrl",
    "sqs:AddPermission",
    "sqs:ListQueues",
    "sqs>DeleteQueue",
    "sqs:GetQueueAttributes",
    "sqs:ListQueueTags",
    "sqs:CreateQueue",
    "sqs:SetQueueAttributes"
  ],
  "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
},
{
  "Sid" : "CloudWatchActions1",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "iam:GetInstanceProfile",
    "cloudwatch>DeleteAlarms",
    "cloudwatch:DescribeAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
    "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
  ]
},
{
  "Sid" : "EfsActions0",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "route53:ListHostedZones",
    "ec2:CreateSecurityGroup",
    "ec2:AuthorizeSecurityGroupIngress",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:CreateFileSystem",
    "elasticfilesystem:CreateMountTarget",
    "elasticfilesystem:DescribeMountTargets",
    "elasticfilesystem:DescribeMountTargetSecurityGroups"
  ],

```

```
    "Resource" : "*"
  },
  {
    "Sid" : "S3Actions1",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::launchwizard*",
      "arn:aws:s3:::launchwizard*/**",
      "arn:aws:s3:::aws-sap-data-provider/config.properties"
    ]
  },
  {
    "Sid" : "CloudFormationActions2",
    "Effect" : "Allow",
    "Action" : "cloudformation:TagResource",
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : "LaunchWizard*"
      }
    }
  },
  {
    "Sid" : "LambdaActions0",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:PutBucketVersioning",
      "s3>DeleteBucket",
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:GetFunction",
      "lambda:GetFunctionConfiguration",
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:LaunchWizard*",
      "arn:aws:s3:::launchwizard*"
    ]
  },
},
```

```
{
  "Sid" : "DynamodbActions0",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:CreateTable",
    "dynamodb:DescribeTable",
    "dynamodb>DeleteTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
},
{
  "Sid" : "SecretsManagerActions0",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource",
    "secretsmanager:UntagResource",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager>DeleteResourcePolicy",
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
},
{
  "Sid" : "SecretsManagerActions1",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SsmActions5",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateOpsMetadata"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SsmActions6",
```

```
    "Effect" : "Allow",
    "Action" : "ssm:DeleteOpsMetadata",
    "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
  },
  {
    "Sid" : "SnsActions0",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:DeleteTopic",
      "sns:Subscribe",
      "sns:Unsubscribe"
    ],
    "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
  },
  {
    "Sid" : "FsxActions0",
    "Effect" : "Allow",
    "Action" : [
      "fsx:UntagResource",
      "fsx:TagResource",
      "fsx>DeleteFileSystem",
      "fsx:ListTagsForResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/Name" : "LaunchWizard*"
      }
    }
  },
  {
    "Sid" : "FsxActions1",
    "Effect" : "Allow",
    "Action" : [
      "fsx:CreateFileSystem"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/Name" : [
          "LaunchWizard*"
        ]
      }
    }
  }
}
```

```

    }
  },
  {
    "Sid" : "FsxActions2",
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ServiceCatalogActions0",
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:CreatePortfolio",
      "servicecatalog:DescribePortfolio",
      "servicecatalog:CreateConstraint",
      "servicecatalog:CreateProduct",
      "servicecatalog:AssociatePrincipalWithPortfolio",
      "servicecatalog:CreateProvisioningArtifact",
      "servicecatalog:TagResource",
      "servicecatalog:UntagResource"
    ],
    "Resource" : [
      "arn:aws:servicecatalog:*:*:*/*",
      "arn:aws:catalog:*:*:*/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SsmActions7",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CreateAssociation",
      "ssm>DeleteAssociation"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
      "arn:aws:ssm:*:*:association/*"
    ],
  },

```



```

    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "EfsActions1",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:UntagResource",
      "elasticfilesystem:TagResource"
    ],
    "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "LogsActions0",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs>DeleteLogGroup",
      "logs:DescribeLogStreams",
      "logs:UntagResource",
      "logs:TagResource",
      "logs>CreateLogGroup",
      "logs>DeleteLogStream",
      "logs:PutLogEvents",
      "logs:GetLogEvents",
      "logs:GetLogDelivery",
      "logs:GetLogGroupFields",
      "logs:GetLogRecord",
      "logs>ListLogDeliveries"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:LaunchWizard*",
      "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {

```

```

        "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
}
},
{
    "Sid" : "LogsActions1",
    "Effect" : "Allow",
    "Action" : "logs:DescribeLogGroups",
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
    }
},
{
    "Sid" : "FsxActions3",
    "Effect" : "Allow",
    "Action" : [
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "launchwizard.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "FsxActions4",
    "Effect" : "Allow",
    "Action" : [
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes"
    ],
    "Resource" : "*",
    "Condition" : {

```

```

    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "launchwizard.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "FsxActions5",
    "Effect" : "Allow",
    "Action" : [
      "fsx:DeleteStorageVirtualMachine",
      "fsx:DeleteVolume"
    ],
    "Resource" : [
      "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
      "arn:aws:fsx:*:*:backup/*",
      "arn:aws:fsx:*:*:volume/*/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "launchwizard.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLexChannelsAccess

AmazonLexChannelsAccesses una [política AWS administrada](#) que: Esta política permite a los clientes llamar al tiempo de ejecución Lex desde los canales

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de enero de 2021 a las 20:12 UTC
- Hora de edición: 13 de enero de 2021 a las 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:ListBots"
      ],
    },
  ],
}
```

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLexFullAccess

AmazonLexFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a Amazon Lex a través de AWS Management Console. También proporciona acceso para crear roles vinculados al Servicio Lex y conceder permisos a Lex para invocar un conjunto limitado de funciones de Lambda.

Uso de esta política

Puede asociar AmazonLexFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de abril de 2017 a las 23:20 UTC
- Hora editada: 7 de febrero de 2024 a las 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    }
  ],
}
```

```

{
  "Sid" : "AmazonLexFullAccessStatement3",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
    "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
    "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
    "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
    "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
  ]
},
{
  "Sid" : "AmazonLexFullAccessStatement4",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "lex.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement5",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
  ]
}

```

```

    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "channels.lex.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement6",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "lexv2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement7",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement8",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ]
  }
}

```



```

    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "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"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonLexReadOnly

AmazonLexReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Amazon Lex.

Uso de esta política

Puede asociar AmazonLexReadOnly a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 11 de abril de 2017 a las 23:13 UTC
- Hora de edición: 31 de enero de 2023 a las 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLexReplicationPolicy

AmazonLexReplicationPolicy es una [política AWS gestionada](#) que: permite a Amazon Lex replicar los recursos de Lex en todas las regiones en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 31 de enero de 2024 a las 23:29 UTC
- Hora editada: 8 de marzo de 2024, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex>DeleteBotAlias",
        "lex:DescribeBotAlias",
```

```
    "lex:CreateBotVersion",
    "lex>DeleteBotVersion",
    "lex:DescribeBotVersion",
    "lex:CreateExport",
    "lex:DescribeBot",
    "lex:UpdateExport",
    "lex:DescribeExport",
    "lex:DescribeBotLocale",
    "lex:DescribeIntent",
    "lex:ListIntents",
    "lex:DescribeSlotType",
    "lex:ListSlotTypes",
    "lex:DescribeSlot",
    "lex:ListSlots",
    "lex:DescribeCustomVocabulary",
    "lex:StartImport",
    "lex:DescribeImport",
    "lex:CreateBot",
    "lex:UpdateBot",
    "lex>DeleteBot",
    "lex:CreateBotLocale",
    "lex:UpdateBotLocale",
    "lex>DeleteBotLocale",
    "lex:CreateIntent",
    "lex:UpdateIntent",
    "lex>DeleteIntent",
    "lex:CreateSlotType",
    "lex:UpdateSlotType",
    "lex>DeleteSlotType",
    "lex:CreateSlot",
    "lex:UpdateSlot",
    "lex>DeleteSlot",
    "lex:CreateCustomVocabulary",
    "lex:UpdateCustomVocabulary",
    "lex>DeleteCustomVocabulary",
    "lex>DeleteBotChannel",
    "lex>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"
        }
    }
}
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonLexRunBotsOnly

AmazonLexRunBotsOnly es una [política administrada por AWS](#) que: brinda acceso a API de conversación de Amazon Lex.

Uso de esta política

Puede asociar AmazonLexRunBotsOnly a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de abril de 2017 a las 23:06 UTC
- Hora de edición: 18 de agosto de 2021 a las 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex>DeleteSession",
        "lex:RecognizeText",
        "lex:RecognizeUtterance",
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLexV2BotPolicy

AmazonLexV2BotPolicy es una [política administrada por AWS](#) que: proporciona a los bots de Lex V2 acceso para llamar a otros servicios AWS en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de enero de 2021 a las 20:10 UTC
- Hora de edición: 13 de enero de 2021 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLookoutEquipmentFullAccess

AmazonLookoutEquipmentFullAccess es una [política administrada por AWS](#) que: otorga acceso total a las operaciones de Amazon Lookout for Equipment

Uso de esta política

Puede asociar AmazonLookoutEquipmentFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 8 de abril de 2021 a las 15:52 UTC
- Hora de edición: 24 de noviembre de 2021 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLookoutEquipmentReadOnlyAccess

AmazonLookoutEquipmentReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Lookout for Equipments

Uso de esta política

Puede asociar AmazonLookoutEquipmentReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 05 de mayo de 2021 a las 16:47 UTC
- Hora de edición: 10 de noviembre de 2022 a las 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLookoutMetricsFullAccess

AmazonLookoutMetricsFullAccess es una [política administrada por AWS](#) que: brinda acceso a todas las acciones de Amazon Lookout for Metrics

Uso de esta política

Puede asociar AmazonLookoutMetricsFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de mayo de 2021 a las 00:43 UTC
- Hora de edición: 7 de mayo de 2021 a las 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*LookoutMetrics*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "lookoutmetrics.amazonaws.com"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLookoutMetricsReadOnlyAccess

AmazonLookoutMetricsReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso a todas las acciones de solo lectura de Amazon Lookout for Metrics

Uso de esta política

Puede asociar AmazonLookoutMetricsReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 7 de mayo de 2021 a las 00:43 UTC
- Hora de edición: 4 de enero de 2022 a las 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLookoutVisionConsoleFullAccess

AmazonLookoutVisionConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Lookout for Vision y acceso limitado a las dependencias de servicio y consola requeridas.

Uso de esta política

Puede asociar AmazonLookoutVisionConsoleFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de mayo de 2021 a las 19:37 UTC
- Hora de edición: 11 de mayo de 2021 a las 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "LookoutVisionFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "lookoutvision:*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:PutBucketVersioning",
      "s3:PutLifecycleConfiguration",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketPublicAccessBlock"
    ],
    "Resource" : "arn:aws:s3:::lookoutvision-*"
  },
  {
    "Sid" : "LookoutVisionConsoleS3BucketAccess",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetBucketLocation",
      "s3:GetBucketVersioning"
    ],
    "Resource" : "arn:aws:s3:::lookoutvision-*"
  },
  {
    "Sid" : "LookoutVisionConsoleS3ObjectAccess",
    "Effect" : "Allow",
    "Action" : [
```

```
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject",
    "s3:AbortMultipartUpload",
    "s3:ListMultipartUploadParts"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*/*"
},
{
  "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
  "Effect" : "Allow",
  "Action" : [
    "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
    "groundtruthlabeling:AssociatePatchToManifestJob",
    "groundtruthlabeling:DescribeConsoleJob"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleDashboardAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleTagSelectorAccess",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetTagKeys",
    "tag:GetTagValues"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases"
  ],
  "Resource" : "*"
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLookoutVisionConsoleReadOnlyAccess

AmazonLookoutVisionConsoleReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Lookout for Vision y acceso limitado a las dependencias de servicio y consola requeridas.

Uso de esta política

Puede asociar AmazonLookoutVisionConsoleReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de mayo de 2021 a las 19:32 UTC
- Hora de edición: 9 de diciembre de 2021 a las 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeTrialDetection",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListTrialDetections",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
```

```
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:GetMetricStatistics"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLookoutVisionFullAccess

AmazonLookoutVisionFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Lookout for Vision y acceso limitado a las dependencias requeridas.

Uso de esta política

Puede asociar AmazonLookoutVisionFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de mayo de 2021 a las 19:24 UTC
- Hora de edición: 11 de mayo de 2021 a las 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonLookoutVisionReadOnlyAccess

AmazonLookoutVisionReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Lookout for Vision y acceso limitado a las dependencias requeridas.

Uso de esta política

Puede asociar AmazonLookoutVisionReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de mayo de 2021 a las 19:11 UTC
- Hora de edición: 9 de diciembre de 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMachineLearningBatchPredictionsAccess

AmazonMachineLearningBatchPredictionsAccess es una [política administrada por AWS](#) que: concede a los usuarios permiso para solicitar predicciones por lotes de Amazon Machine Learning.

Uso de esta política

Puede asociar AmazonMachineLearningBatchPredictionsAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de abril de 2015 a las 17:12 UTC
- Hora de edición: 9 de abril de 2015 a las 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMachineLearningCreateOnlyAccess

AmazonMachineLearningCreateOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de creación a recursos no predictivos de Amazon Machine Learning.

Uso de esta política

Puede asociar AmazonMachineLearningCreateOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de abril de 2015 a las 17:18 UTC
- Hora de edición: 29 de junio de 2016 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMachineLearningFullAccess

AmazonMachineLearningFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a los recursos de Amazon Machine Learning.

Uso de esta política

Puede asociar AmazonMachineLearningFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de abril de 2015 a las 17:25 UTC
- Hora de edición: 9 de abril de 2015 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

AmazonMachineLearningManageRealTimeEndpointOnlyAccess es una [política administrada por AWS](#) que: concede a los usuarios permiso para crear y eliminar el punto de conexión en tiempo real para los modelos de Amazon Machine Learning.

Uso de esta política

Puede asociar AmazonMachineLearningManageRealTimeEndpointOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de abril de 2015 a las 17:32 UTC
- Hora de edición: 9 de abril de 2015 a las 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMachineLearningReadOnlyAccess

AmazonMachineLearningReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a los recursos de Amazon Machine Learning.

Uso de esta política

Puede asociar AmazonMachineLearningReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de abril de 2015 a las 17:40 UTC
- Hora de edición: 9 de abril de 2015 a las 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

AmazonMachineLearningRealTimePredictionOnlyAccess es una [política administrada por AWS](#) que: concede a los usuarios permiso para solicitar predicciones en tiempo real de Amazon Machine Learning.

Uso de esta política

Puede asociar AmazonMachineLearningRealTimePredictionOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de abril de 2015 a las 17:44 UTC
- Hora de edición: 9 de abril de 2015 a las 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "machinelearning:Predict"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

AmazonMachineLearningRoleforRedshiftDataSourceV3 es una [política administrada por AWS](#) que: permite a Machine Learning configurar y utilizar los clústeres de Redshift y las ubicaciones de almacenamiento provisional de S3 para Redshift Data Source.

Uso de esta política

Puede asociar AmazonMachineLearningRoleforRedshiftDataSourceV3 a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de junio de 2020 a las 18:00 UTC
- Hora de edición: 24 de junio de 2020 a las 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupIngress",
        "redshift:AuthorizeClusterSecurityGroupIngress",
        "redshift:CreateClusterSecurityGroup",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:ModifyCluster",
        "redshift:RevokeClusterSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::amazon-machine-learning*"
    }
  ]
}
```

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMacieFullAccess

AmazonMacieFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Macie.

Uso de esta política

Puede asociar AmazonMacieFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de agosto de 2017 a las 14:54 UTC
- Hora de edición: 1 de julio de 2022 a las 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "pricing:GetProducts",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMacieHandshakeRole

AmazonMacieHandshakeRole es una [política administrada por AWS](#) que: concede permiso para crear el rol vinculado al servicio de Amazon Macie.

Uso de esta política

Puede asociar AmazonMacieHandshakeRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de junio de 2018 a las 15:46 UTC
- Hora de edición: 28 de junio de 2018 a las 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMacieReadOnlyAccess

AmazonMacieReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Macie.

Uso de esta política

Puede asociar AmazonMacieReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de junio de 2023 a las 21:50 UTC
- Hora de edición: 15 de junio de 2023 a las 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMacieServiceRole

AmazonMacieServiceRole es una [política administrada por AWS](#) que: concede a acceso de solo lectura a las dependencias de recursos de la cuenta, para hacer posible el análisis de datos.

Uso de esta política

Puede asociar AmazonMacieServiceRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 14:53 UTC
- Hora de edición: 14 de agosto de 2017 a las 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMacieServiceRolePolicy

AmazonMacieServiceRolePolicy es una [política administrada por AWS](#) que: se encuentra vinculada al servicio para Amazon Macie

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de junio de 2018 a las 22:17 UTC
- Hora de edición: 19 de mayo de 2022 a las 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "organizations:DescribeAccount",
    "organizations:ListAccounts",
    "s3:GetAccountPublicAccessBlock",
    "s3:ListAllMyBuckets",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListBucket",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectTagging"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/macie/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
  ]
}
]

```

```
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonManagedBlockchainConsoleFullAccess

AmazonManagedBlockchainConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Managed Blockchain a través del AWS Management Console

Uso de esta política

Puede asociar AmazonManagedBlockchainConsoleFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de abril de 2019 a las 21:23 UTC
- Hora de edición: 29 de abril de 2019 a las 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "managedblockchain:*",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:CreateVpcEndpoint",
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonManagedBlockchainFullAccess

AmazonManagedBlockchainFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Managed Blockchain.

Uso de esta política

Puede asociar AmazonManagedBlockchainFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS

- Hora de creación: 29 de abril de 2019 a las 21:39 UTC
- Hora de edición: 29 de abril de 2019 a las 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonManagedBlockchainReadOnlyAccess

AmazonManagedBlockchainReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Managed Blockchain.

Uso de esta política

Puede asociar AmazonManagedBlockchainReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de abril de 2019 a las 18:17 UTC
- Hora de edición: 30 de abril de 2019 a las 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonManagedBlockchainServiceRolePolicy

AmazonManagedBlockchainServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y los recursos utilizados o administrados por Amazon Managed Blockchain

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de enero de 2020 a las 19:51 UTC
- Hora de edición: 17 de enero de 2020 a las 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMCSFullAccess

AmazonMCSFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo al servicio Apache Cassandra administrado por Amazon

Uso de esta política

Puede asociar AmazonMCSFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 13:45 UTC
- Hora de edición: 17 de abril de 2020 a las 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling>DeleteScheduledAction",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    }
  ]
}
```

```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMCSReadOnlyAccess

AmazonMCSReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio Apache Cassandra administrado por Amazon

Uso de esta política

Puede asociar AmazonMCSReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 13:46 UTC
- Hora de edición: 17 de abril de 2020 a las 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Action" : [
  "application-autoscaling:DescribeScalableTargets",
  "application-autoscaling:DescribeScalingActivities",
  "application-autoscaling:DescribeScalingPolicies",
  "application-autoscaling:DescribeScheduledActions",
  "cloudwatch:DescribeAlarms"
],
"Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMechanicalTurkFullAccess

AmazonMechanicalTurkFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todas las API de Amazon Mechanical Turk.

Uso de esta política

Puede asociar AmazonMechanicalTurkFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de diciembre de 2015 a las 19:08 UTC
- Hora de edición: 11 de diciembre de 2015 a las 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMechanicalTurkReadOnly

AmazonMechanicalTurkReadOnly es una [política administrada por AWS](#) que: proporciona acceso a las API de solo lectura en Amazon Mechanical Turk.

Uso de esta política

Puede asociar `AmazonMechanicalTurkReadOnly` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de diciembre de 2015 a las 19:08 UTC
- Hora de edición: 25 de septiembre de 2019 a las 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMemoryDBFullAccess

AmazonMemoryDBFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a Amazon MemoryDB a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonMemoryDBFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de octubre de 2021 a las 19:24 UTC
- Hora de edición: 8 de octubre de 2021 a las 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```



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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMemoryDBReadOnlyAccess

AmazonMemoryDBReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon MemoryDB a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonMemoryDBReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de octubre de 2021 a las 19:27 UTC
- Hora de edición: 8 de octubre de 2021 a las 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMobileAnalyticsFinancialReportAccess

AmazonMobileAnalyticsFinancialReportAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a todos los informes, incluidos los datos financieros, de todos los recursos de la aplicación.

Uso de esta política

Puede asociar AmazonMobileAnalyticsFinancialReportAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "mobileanalytics:GetReports",
        "mobileanalytics:GetFinancialReports"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMobileAnalyticsFullAccess

AmazonMobileAnalyticsFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a todos los recursos de la aplicación.

Uso de esta política

Puede asociar AmazonMobileAnalyticsFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMobileAnalyticsNon-financialReportAccess

AmazonMobileAnalyticsNon-financialReportAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a informes no financieros para todos los recursos de la aplicación.

Uso de esta política

Puede asociar AmazonMobileAnalyticsNon-financialReportAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMobileAnalyticsWriteOnlyAccess

AmazonMobileAnalyticsWriteOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo escritura para colocar los datos de eventos de todos los recursos de la aplicación. (Se recomienda para la integración del SDK)

Uso de esta política

Puede asociar AmazonMobileAnalyticsWriteOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMonitronFullAccess

AmazonMonitronFullAccess es una [política administrada por AWS](#) que: proporciona acceso total para gestionar Amazon Monitron

Uso de esta política

Puede asociar AmazonMonitronFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de diciembre de 2020 a las 22:40 UTC
- Hora de edición: 8 de junio de 2022 a las 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "monitron.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "monitron:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:ListKeys",
      "kms:DescribeKey",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "kms:CreateGrant",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "monitron.*.amazonaws.com"
        ]
      },
      "Bool" : {
        "kms:GrantIsForAWSResource" : true
      }
    }
  },
  {
    "Sid" : "AWSSS0Permissions",
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMQApiFullAccess

AmazonMQApiFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AmazonMQ a través de nuestra API/SDK.

Uso de esta política

Puede asociar AmazonMQApiFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de diciembre de 2018 a las 20:31 UTC
- Hora de edición: 4 de noviembre de 2020 a las 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
```

```

    "ec2:DescribeInternetGateways",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeNetworkInterfacePermissions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
  ]
},
{
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "mq.amazonaws.com"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMQApiReadOnlyAccess

AmazonMQApiReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AmazonMQ a través de nuestra API/SDK.

Uso de esta política

Puede asociar AmazonMQApiReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de diciembre de 2018 a las 20:31 UTC
- Hora de edición: 18 de diciembre de 2018 a las 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
    }
  ]
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMQFullAccess

AmazonMQFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AmazonMQ a través del AWS Management Console.

Uso de esta política

Puede asociar AmazonMQFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2017 a las 15:28 UTC
- Hora de edición: 4 de noviembre de 2020 a las 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
} ]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMQReadOnlyAccess

AmazonMQReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AmazonMQ a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonMQReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2017 a las 15:30 UTC
- Hora de edición: 28 de noviembre de 2017 a las 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMQServiceRolePolicy

AmazonMQServiceRolePolicy es una [política administrada por AWS](#) que: tiene roles vinculados a servicios para Amazon MQ AWS

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de noviembre de 2020 a las 16:07 UTC
- Hora de edición: 4 de noviembre de 2020 a las 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",

```

```
    "arn:aws:ec2:*:*:security-group/*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/AMQManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AMQManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
    "logs:PutLogEvents",
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups",
    "logs:CreateLogStream",
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
  ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMSKConnectReadOnlyAccess

AmazonMSKConnectReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon MSK Connect

Uso de esta política

Puede asociar AmazonMSKConnectReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de septiembre de 2021 a las 10:18 UTC
- Hora de edición: 18 de octubre de 2021 a las 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeConnector"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:connector/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeCustomPlugin"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:custom-plugin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeWorkerConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:worker-configuration/*"
      ]
    }
  ]
}
```

```
    ]  
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMSKFullAccess

AmazonMSKFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon MSK y otros permisos necesarios para sus dependencias.

Uso de esta política

Puede asociar AmazonMSKFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de enero de 2019 a las 22:07 UTC
- Hora de edición: 18 de octubre de 2023 a las 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:*",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group*"
      ]
    }
  ],
  {
    "Effect" : "Allow",
```

```
"Action" : [
  "ec2:CreateVpcEndpoint"
],
"Resource" : [
  "arn:*:ec2:*:*:vpc-endpoint/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:RequestTag/AWSMSKManaged" : "true"
  },
  "StringLike" : {
    "aws:RequestTag/ClusterArn" : "*"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AWSMSKManaged" : "true"
    },
    "StringLike" : {
      "ec2:ResourceTag/ClusterArn" : "*"
    }
  }
},
{
  "Effect" : "Allow",
```



```

    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "kafka.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "kafka.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMSKReadOnlyAccess

AmazonMSKReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon MSK

Uso de esta política

Puede asociar AmazonMSKReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de enero de 2019 a las 22:28 UTC
- Hora de edición: 14 de enero de 2019 a las 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
      ]
    }
  ]
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonMWAAServiceRolePolicy

AmazonMWAAServiceRolePolicy es una [política administrada por AWS](#) que: tiene un rol vinculado a servicios utilizado por Amazon Managed Workflows para Apache Airflow.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de noviembre de 2020 a las 14:13 UTC
- Hora de edición: 17 de noviembre de 2022 a las 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    }
  ]
}
```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonMWAAManaged" : false
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "AmazonMWAAManaged"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",

```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/MWAA"
        ]
      }
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonNimbleStudio-LaunchProfileWorker

AmazonNimbleStudio-LaunchProfileWorker es una [política administrada por AWS](#) que otorga acceso a los recursos que necesitan los trabajadores de Nimble Studio Launch Profile. Adjunte esta política a las instancias de EC2 creadas por Nimble Studio Builder.

Uso de esta política

Puede asociar AmazonNimbleStudio-LaunchProfileWorker a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de abril de 2021 a las 4:47 UTC
- Hora de edición: 28 de abril de 2021 a las 4:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      },
      "Sid" : "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version" : "2012-10-17"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonNimbleStudio-StudioAdmin

AmazonNimbleStudio-StudioAdmin es una [política administrada por AWS](#) que: otorga acceso a los recursos de Amazon Nimble Studio asociados al administrador del estudio y a los recursos del estudio relacionados en otros servicios. Adjunte esta política al rol de administrador asociado a su estudio.

Uso de esta política

Puede asociar AmazonNimbleStudio-StudioAdmin a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de abril de 2021 a las 4:47 UTC
- Hora de edición: 22 de septiembre de 2023 a las 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",

```



```

    "nimble:GetStreamingSessionStream",
    "nimble>DeleteStreamingSession",
    "nimble:ListStreamingSessionBackups",
    "nimble:GetStreamingSessionBackup",
    "nimble:ListEulas",
    "nimble:ListEulaAcceptances",
    "nimble:GetEula",
    "nimble:AcceptEulas",
    "nimble:ListStudioMembers",
    "nimble:GetStudioMember",
    "nimble:ListStreamingSessions",
    "nimble:GetStreamingImage",
    "nimble:ListStreamingImages",
    "nimble:GetLaunchProfileInitialization",
    "nimble:GetLaunchProfileDetails",
    "nimble:GetFeatureMap",
    "nimble:PutStudioLogEvents",
    "nimble:ListLaunchProfiles",
    "nimble:GetLaunchProfile",
    "nimble:GetLaunchProfileMember",
    "nimble:ListLaunchProfileMembers",
    "nimble:PutLaunchProfileMembers",
    "nimble:UpdateLaunchProfileMember",
    "nimble>DeleteLaunchProfileMember"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sso-directory:DescribeUsers",
    "sso-directory:SearchUsers",
    "identitystore:DescribeUser",
    "identitystore:ListUsers"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ds:CreateComputer",
    "ds:DescribeDirectories",

```

```
    "ec2:DescribeSubnets",
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2>DeleteNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2:DescribeSecurityGroups",
    "fsx:DescribeFileSystems"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "nimble.amazonaws.com"
    }
  }
}
],
"Version" : "2012-10-17"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonNimbleStudio-StudioUser

AmazonNimbleStudio-StudioUser es una [política administrada por AWS](#) que: otorga acceso a los recursos de Amazon Nimble Studio asociados al usuario del estudio y a los recursos del estudio relacionados en otros servicios. Adjunte esta política al rol de usuario asociado a su estudio.

Uso de esta política

Puede asociar AmazonNimbleStudio-StudioUser a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de abril de 2021 a las 4:48 UTC
- Hora de edición: 22 de septiembre de 2023 a las 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sso-directory:DescribeUsers",
      "sso-directory:SearchUsers",
      "identitystore:DescribeUser",
      "identitystore:ListUsers"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "nimble:ListLaunchProfiles"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "nimble:requesterPrincipalId" : "${nimble:principalId}"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "nimble:ListStudioMembers",
      "nimble:GetStudioMember",
      "nimble:ListEulas",
      "nimble:ListEulaAcceptances",
      "nimble:GetFeatureMap",
      "nimble:PutStudioLogEvents"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "nimble>DeleteStreamingSession",
      "nimble:GetStreamingSession",
      "nimble:StartStreamingSession",

```

```
    "nimble:StopStreamingSession",
    "nimble>CreateStreamingSessionStream",
    "nimble:GetStreamingSessionStream",
    "nimble>ListStreamingSessions",
    "nimble>ListStreamingSessionBackups",
    "nimble:GetStreamingSessionBackup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
    }
  }
}
],
"Version" : "2012-10-17"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOmicsFullAccess

AmazonOmicsFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Omics y otros requisitos obligatorios de Servicios de AWS. Esta política permite al usuario ver y aceptar las invitaciones a compartir RAM para acceder a recursos ajenos a los del usuario Cuenta de AWS.

Uso de esta política

Puede asociar AmazonOmicsFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de febrero de 2023 a las 00:59 UTC
- Hora de edición: 24 de febrero de 2023 a las 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "omics.amazonaws.com"
    }
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOmicsReadOnlyAccess

AmazonOmicsReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Omics

Uso de esta política

Puede asociar AmazonOmicsReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2022 a las 4:17 UTC
- Hora de edición: 29 de noviembre de 2022 a las 4:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOneEnterpriseFullAccess

AmazonOneEnterpriseFullAccesses una [política AWS gestionada](#) que: Esta política concede permisos administrativos que permiten el acceso a todos los recursos y operaciones de Amazon One Enterprise.

Uso de la política

Puede asociar `AmazonOneEnterpriseFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2023 a las 04:58 UTC
- Hora editada: 28 de noviembre de 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOneEnterpriseInstallerAccess

AmazonOneEnterpriseInstallerAccesses una [política AWS administrada](#) que: Esta política otorga permisos de lectura y escritura limitados que permiten la instalación y activación del dispositivo.

Uso de la política

Puede asociar AmazonOneEnterpriseInstallerAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2023 a las 05:00 UTC
- Hora editada: 28 de noviembre de 2023 a las 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "one:CreateDeviceActivationQrCode",
  "one:GetDeviceInstance",
  "one:GetSite",
  "one:GetSiteAddress",
  "one:ListDeviceInstances",
  "one:ListSites"
],
"Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOneEnterpriseReadOnlyAccess

AmazonOneEnterpriseReadOnlyAccesses una [política AWS gestionada](#) que: Esta política concede permisos de solo lectura a todos los recursos y operaciones de Amazon One Enterprise.

Uso de la política

Puede asociar AmazonOneEnterpriseReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2023 a las 04:59 UTC
- Hora editada: 28 de noviembre de 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchDashboardsServiceRolePolicy

AmazonOpenSearchDashboardsServiceRolePolicy es una [política AWS gestionada](#) que: proporciona acceso al servicio Amazon OpenSearch Dashboards para acceder a otros AWS servicios, por ejemplo, CloudWatch en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de diciembre de 2023 a las 19:38 UTC
- Hora editada: 22 de diciembre de 2023 a las 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchIngestionFullAccess

AmazonOpenSearchIngestionFullAccess es una [política administrada por AWS](#) que: permite a Amazon OpenSearch Ingestion acceder a otros servicios de AWS en su nombre.

Uso de esta política

Puede asociar AmazonOpenSearchIngestionFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de abril de 2023 a las 18:11 UTC
- Hora de edición: 26 de abril de 2023 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "osis:CreatePipeline",
      "osis:UpdatePipeline",
      "osis>DeletePipeline",
      "osis:StartPipeline",
      "osis:StopPipeline",
      "osis:ListPipelines",
      "osis:GetPipeline",
      "osis:GetPipelineChangeProgress",
      "osis:ValidatePipeline",
      "osis:GetPipelineBlueprint",
      "osis:ListPipelineBlueprints",
      "osis:TagResource",
      "osis:UntagResource",
      "osis:ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "osis.amazonaws.com"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchIngestionReadOnlyAccess

AmazonOpenSearchIngestionReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio Amazon OpenSearch Ingestion

Uso de esta política

Puede asociar AmazonOpenSearchIngestionReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de abril de 2023 a las 18:09 UTC
- Hora de edición: 26 de abril de 2023 a las 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchIngestionServiceRolePolicy

AmazonOpenSearchIngestionServiceRolePolicy es una [política administrada por AWS](#) que permite a Amazon OpenSearch Ingestion Service acceder a otros servicios de AWS en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2022 a las 16:49 UTC
- Hora de edición: 18 de noviembre de 2022 a las 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteVpcEndpoints"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/OSISManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/OSIS"
    }
  }
}
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchServerlessServiceRolePolicy

AmazonOpenSearchServerlessServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon OpenSearch sin servidor acceder a otros servicios de AWS, como las API de CloudWatch, en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de noviembre de 2022 a las 19:50 UTC
- Hora de edición: 24 de noviembre de 2022 a las 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchServiceCognitoAccess

AmazonOpenSearchServiceCognitoAccess es una [política administrada por AWS](#) que proporciona acceso al servicio de configuración de Amazon Cognito.

Uso de esta política

Puede asociar AmazonOpenSearchServiceCognitoAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de septiembre de 2021 a las 6:31 UTC
- Hora de edición: 20 de diciembre de 2021 a las 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp>DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : [
        "arn:aws:cognito-identity:*:*:identitypool/*",
        "arn:aws:cognito-idp:*:*:userpool/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam:*:*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "cognito-identity:SetIdentityPoolRoles",
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchServiceFullAccess

AmazonOpenSearchServiceFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo al servicio de configuración de Amazon OpenSearch Service.

Uso de esta política

Puede asociar AmazonOpenSearchServiceFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de septiembre de 2021 a las 5:33 UTC
- Hora de edición: 8 de septiembre de 2021 a las 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchServiceReadOnlyAccess

AmazonOpenSearchServiceReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio de configuración de Amazon OpenSearch Service.

Uso de esta política

Puede asociar `AmazonOpenSearchServiceReadOnlyAccess` a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de septiembre de 2021 a las 5:38 UTC
- Hora de edición: 8 de septiembre de 2021 a las 5:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonOpenSearchServiceRolePolicy

AmazonOpenSearchServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon OpenSearch Service acceder en su nombre a otros servicios de AWS, como las API de red de EC2.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de agosto de 2021 a las 9:27 UTC
- Hora de edición: 23 de octubre de 2023 a las 7:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2>DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
```

```
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Sid" : "Stmt1480452973149",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973150",
  "Effect" : "Allow",
  "Action" : [
    "ec2:UnAssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973154",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973164",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973174",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
```

```
"Sid" : "Stmt1480452973184",
"Effect" : "Allow",
"Action" : [
  "elasticloadbalancing:AddListenerCertificates",
  "elasticloadbalancing:RemoveListenerCertificates"
],
"Resource" : [
  "arn:aws:elasticloadbalancing:*:*:listener/*"
]
},
{
  "Sid" : "Stmt1480452973194",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ]
},
{
  "Sid" : "Stmt1480452973195",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeTags"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973196",
  "Effect" : "Allow",
  "Action" : [
    "acm:DescribeCertificate"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973197",
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/ES"
    }
  }
}
```

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonPersonalizeFullAccess

AmazonPersonalizeFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Personalize mediante AWS Management Console y SDK. También proporciona acceso selecto a servicios relacionados (por ejemplo, S3, CloudWatch).

Uso de esta política

Puede asociar AmazonPersonalizeFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de diciembre de 2018 a las 22:24 UTC
- Hora de edición: 30 de mayo de 2019 a las 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "personalize:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
```



```
    "s3:DeleteObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::*Personalize*",
    "arn:aws:s3:::*personalize*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "personalize.amazonaws.com"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonPollyFullAccess

AmazonPollyFullAccess es una [política administrada por AWS](#) que: otorga acceso total al servicio y los recursos de Amazon Polly.

Uso de esta política

Puede asociar AmazonPollyFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2016 a las 18:59 UTC
- Hora de edición: 30 de noviembre de 2016 a las 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonPollyReadOnlyAccess

AmazonPollyReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura a los recursos de Amazon Polly.

Uso de esta política

Puede asociar AmazonPollyReadOnlyAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2016 a las 18:59 UTC
- Hora de edición: 17 de julio de 2018 a las 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "polly:GetSpeechSynthesisTask",
    "polly:ListLexicons",
    "polly:ListSpeechSynthesisTasks",
    "polly:SynthesizeSpeech"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonPrometheusConsoleFullAccess

AmazonPrometheusConsoleFullAccess es una [política administrada por AWS](#) que: otorga acceso total a los recursos AWS Managed Prometheus en la consola AWS

Uso de esta política

Puede asociar AmazonPrometheusConsoleFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 18:11 UTC
- Hora de edición: 24 de octubre de 2022 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
        "aps>DeleteWorkspace",
        "aps>ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps>CreateAlertManagerDefinition",
        "aps>CreateRuleGroupsNamespace",
        "aps>DeleteAlertManagerDefinition",
        "aps>DeleteRuleGroupsNamespace",
        "aps>ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps>CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps>DeleteLoggingConfiguration",
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonPrometheusFullAccess

AmazonPrometheusFullAccess es una [política administrada por AWS](#) que: otorga acceso total a los recursos AWS Managed Prometheus

Uso de esta política

Puede asociar AmazonPrometheusFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 18:10 UTC
- Hora editada: 26 de noviembre de 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scrapper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scrapper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}
  }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonPrometheusQueryAccess

AmazonPrometheusQueryAccess es una [política administrada por AWS](#) que: brinda acceso para ejecutar consultas en los recursos AWS Managed Prometheus

Uso de esta política

Puede asociar AmazonPrometheusQueryAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de diciembre de 2020 a la 1:02 UTC
- Hora de edición: 19 de diciembre de 2020 a la 1:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonPrometheusRemoteWriteAccess

AmazonPrometheusRemoteWriteAccess es una [política administrada por AWS](#) que: concede acceso de solo escritura a los espacios de trabajo AWS Managed Prometheus

Uso de esta política

Puede asociar AmazonPrometheusRemoteWriteAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de diciembre de 2020 a las 1:04 UTC
- Hora de edición: 19 de diciembre de 2020 a las 1:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonPrometheusScraperserviceRolePolicy

AmazonPrometheusScraperserviceRolePolicy es una [política AWS gestionada](#) que: proporciona acceso a AWS los recursos gestionados o utilizados por Amazon Managed Service for Prometheus Collector

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2023 a las 14:19 UTC
- Hora editada: 26 de noviembre de 2023 a las 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperserviceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/scrapper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScrapper*"
  },
  {
    "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}"
    }
  }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonQFullAccess

AmazonQFullAccesses una [política AWS gestionada](#) que: proporciona acceso total para permitir las interacciones con Amazon Q

Uso de la política

Puede asociar AmazonQFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2023 a las 16:00 UTC
- Hora editada: 28 de noviembre de 2023 a las 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonQLDBConsoleFullAccess

AmazonQLDBConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon QLDB a través de AWS Management Console.

Uso de esta política

Puede asociar AmazonQLDBConsoleFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de septiembre de 2019 a las 18:24 UTC
- Hora de edición: 4 de noviembre de 2022 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "qldb:UpdateLedger",
    "qldb:UpdateLedgerPermissionsMode",
    "qldb>DeleteLedger",
    "qldb:ListLedgers",
    "qldb:DescribeLedger",
    "qldb:ExportJournalToS3",
    "qldb:ListJournalS3Exports",
    "qldb:ListJournalS3ExportsForLedger",
    "qldb:DescribeJournalS3Export",
    "qldb:CancelJournalKinesisStream",
    "qldb:DescribeJournalKinesisStream",
    "qldb:ListJournalKinesisStreamsForLedger",
    "qldb:StreamJournalToKinesis",
    "qldb:GetBlock",
    "qldb:GetDigest",
    "qldb:GetRevision",
    "qldb:TagResource",
    "qldb:UntagResource",
    "qldb:ListTagsForResource",
    "qldb:SendCommand",
    "qldb:ExecuteStatement",
    "qldb:ShowCatalog",
    "qldb:InsertSampleData",
    "qldb:PartiQLCreateTable",
    "qldb:PartiQLCreateIndex",
    "qldb:PartiQLDropTable",
    "qldb:PartiQLDropIndex",
    "qldb:PartiQLUndropTable",
    "qldb:PartiQLDelete",
    "qldb:PartiQLInsert",
    "qldb:PartiQLUpdate",
    "qldb:PartiQLSelect",
    "qldb:PartiQLHistoryFunction",
    "qldb:PartiQLRedact"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "dbqms:*"
  ],
  "Resource" : "*"
},
},

```



```
{
  "Effect" : "Allow",
  "Action" : [
    "kinesis:ListStreams",
    "kinesis:DescribeStream"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "qldb.amazonaws.com"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonQLDBFullAccess

AmazonQLDBFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon QLDB a través de la API de servicio.

Uso de esta política

Puede asociar AmazonQLDBFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de septiembre de 2019 a las 18:23 UTC
- Hora de edición: 4 de noviembre de 2022 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb>DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:GetBlock",

```

```

    "qldb:TagResource",
    "qldb:UntagResource",
    "qldb:ListTagsForResource",
    "qldb:SendCommand",
    "qldb:PartiQLCreateTable",
    "qldb:PartiQLCreateIndex",
    "qldb:PartiQLDropTable",
    "qldb:PartiQLDropIndex",
    "qldb:PartiQLUndropTable",
    "qldb:PartiQLDelete",
    "qldb:PartiQLInsert",
    "qldb:PartiQLUpdate",
    "qldb:PartiQLSelect",
    "qldb:PartiQLHistoryFunction",
    "qldb:PartiQLRedact"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "qldb.amazonaws.com"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonQLDBReadOnly

AmazonQLDBReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon QLDB.

Uso de esta política

Puede asociar AmazonQLDBReadOnly a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de septiembre de 2019 a las 18:19 UTC
- Hora de edición: 2 de julio de 2021 a las 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeJournalKinesisStream",

```

```
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListTagsForResource"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSBetaServiceRolePolicy

AmazonRDSBetaServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon RDS gestionar los recursos AWS en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de mayo de 2018 a las 19:41 UTC
- Hora de edición: 14 de diciembre de 2022 a las 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteCoipPoolPermission",
        "ec2>DeleteLocalGatewayRouteTablePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
```

```
    "ec2:RevokeSecurityGroupIngress",
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeVpcEndpoints",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "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"
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSCustomInstanceProfileRolePolicy

AmazonRDSCustomInstanceProfileRolePolicy es una [política AWS gestionada](#) que: permite a Amazon RDS Custom realizar diversas acciones de automatización y tareas de administración de bases de datos a través de un perfil de instancia EC2.

Uso de la política

Puede asociar AmazonRDSCustomInstanceProfileRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 27 de febrero de 2024 a las 17:42 UTC
- Hora editada: 27 de febrero de 2024 a las 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

```
  },
  {
    "Sid" : "ssmAgentPermission4",
    "Effect" : "Allow",
    "Action" : [
      "ssmmessages:CreateControlChannel",
      "ssmmessages:OpenControlChannel"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ssmAgentPermission5",
    "Effect" : "Allow",
    "Action" : [
      "ec2messages:AcknowledgeMessage",
      "ec2messages:DeleteMessage",
      "ec2messages:FailMessage",
      "ec2messages:GetEndpoint",
      "ec2messages:GetMessages",
      "ec2messages:SendReply"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "createEc2SnapshotPermission1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot",
      "ec2:CreateSnapshots"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {

```

```
"Sid" : "createEc2SnapshotPermission2",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateSnapshot",
  "ec2:CreateSnapshots"
],
"Resource" : [
  "arn:aws:ec2:*::snapshot/*"
],
"Condition" : {
  "StringLike" : {
    "aws:RequestTag/AWSRDSCustom" : [
      "custom-oracle",
      "custom-sqlserver",
      "custom-oracle-rac"
    ]
  }
},
{
  "Sid" : "createEc2SnapshotPermission3",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : [
    "arn:aws:ec2:*::instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "createTagForEc2SnapshotPermission",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
```

```

        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
    ],
    "ec2:CreateAction" : [
        "CreateSnapshot",
        "CreateSnapshots"
    ]
}
},
{
    "Sid" : "rdsCustomS3ObjectPermission",
    "Effect" : "Allow",
    "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
    ],
    "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "rdsCustomS3BucketPermission",
    "Effect" : "Allow",
    "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
    ],
    "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
}

```

```

    }
  },
  {
    "Sid" : "readSecretsFromCpPermission",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue",
      "secretsmanager:DescribeSecret"
    ],
    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "createSecretsOnDpPermission",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:TagResource"
    ],
    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
      }
    }
  },
  {
    "Sid" : "publishCwMetricsPermission",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {

```

```

    "StringEquals" : {
      "cloudwatch:namespace" : [
        "rdscustom/rds-custom-sqlserver-agent",
        "RDSCustomForOracle/Agent"
      ]
    }
  },
  {
    "Sid" : "putEventsToEventBusPermission",
    "Effect" : "Allow",
    "Action" : "events:PutEvents",
    "Resource" : "arn:aws:events:*:*:event-bus/default"
  },
  {
    "Sid" : "cwlUploadPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutRetentionPolicy",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams",
      "logs:CreateLogStream",
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
  },
  {
    "Sid" : "sendMessageToSqsQueuePermission",
    "Effect" : "Allow",
    "Action" : [
      "sqs:SendMessage",
      "sqs:ReceiveMessage",
      "sqs>DeleteMessage",
      "sqs:GetQueueUrl"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
      }
    }
  }
},

```

```

{
  "Sid" : "managePrivateIpOnEniPermission",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses",
    "ec2:UnassignPrivateIpAddresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
    }
  }
},
{
  "Sid" : "kmsPermissionWithSecret",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
    },
    "StringLike" : {
      "kms:ViaService" : "secretsmanager.*.amazonaws.com"
    }
  }
},
{
  "Sid" : "kmsPermissionWithS3",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
* "

```



```
    },
    "StringLike" : {
      "kms:ViaService" : "s3.*.amazonaws.com"
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonRDSCustomPreviewServiceRolePolicy

AmazonRDSCustomPreviewServiceRolePolicy es una [política administrada por AWS](#) que sirve como política de rol de servicio preliminar de Amazon RDS Custom

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de octubre de 2021 a las 21:44 UTC
- Hora de edición: 20 de septiembre de 2023 a las 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
```

```
        "*"
    ]
},
{
    "Sid" : "ecc2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "ecc1scoping",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AllocateAddress"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:RequestTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
}
```

```
  },
  {
    "Sid" : "ecc1scoping2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssociateAddress",
      "ec2:DisassociateAddress",
      "ec2:ReleaseAddress"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "ecc1scoping3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssignPrivateIpAddresses"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances1",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*",
```

```

    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
    "arn:aws:ec2:*:*:placement-group*"
  ]
},
{
  "Sid" : "eccRunInstances3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:snapshot*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac",
        "custom-oracle"
      ]
    }
  }
}
}

```

```
  },
  {
    "Sid" : "RequireImdsV2",
    "Effect" : "Deny",
    "Action" : "ec2:RunInstances",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringNotEquals" : {
        "ec2:MetadataHttpTokens" : "required"
      },
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances3keyPair1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2>DeleteKeyPair"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
    ],
    "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" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSCustomServiceRolePolicy

AmazonRDSCustomServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon RDS Custom gestionar los recursos AWS en su nombre.

Uso de esta política

Esta política está adjunta a un rol vinculado a servicios que permite al servicio realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Detalles de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de octubre de 2021 a las 21:39 UTC
- Hora de edición: 20 de septiembre de 2023 a las 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
```

```

    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeVolumes",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeIamInstanceProfileAssociations",
    "ec2:DescribeImages",
    "ec2:DescribeVpcs",
    "ec2:RegisterImage",
    "ec2:DeregisterImage",
    "ec2:DescribeTags",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVolumesModifications",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:SearchTransitGatewayMulticastGroups",
    "ec2:GetTransitGatewayMulticastDomainAssociations",
    "ec2:DescribeTransitGatewayMulticastDomains",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeRouteTables"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ecc2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation",
    "ec2:TerminateInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:RebootInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
}

```

```
    ]
  }
}
},
{
  "Sid" : "ecc1scoping",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ecc1scoping2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
},
```

```
{
  "Sid" : "ecc1scoping3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances1",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:image/*",
```

```

    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
    "arn:aws:ec2:*:*:placement-group/*"
  ]
},
{
  "Sid" : "eccRunInstances3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac",
        "custom-oracle"
      ]
    }
  }
},
{
  "Sid" : "RequireImdsV2",
  "Effect" : "Deny",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringNotEquals" : {
      "ec2:MetadataHttpTokens" : "required"
    },
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances3keyPair1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",

```

```

    "ec2:DeleteKeyPair"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
  ],
  "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" : "*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSDDataFullAccess

AmazonRDSDDataFullAccess es una [política administrada por AWS](#) que: permite el acceso total para utilizar las API de datos de RDS, las API de almacenamiento secreto para las credenciales de las bases de datos de RDS y las API de administración de consultas de la consola de base de datos para ejecutar sentencias SQL en los clústeres de Aurora sin servidor de Cuenta de AWS.

Uso de esta política

Puede asociar AmazonRDSDDataFullAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de noviembre de 2018 a las 21:29 UTC

- Hora de edición: 20 de noviembre de 2019 a las 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
    },
    {
      "Sid" : "RDSDataServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms>DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms>CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",

```

```
        "dbqms:DeleteQueryHistory",
        "rds-data:ExecuteSql",
        "rds-data:ExecuteStatement",
        "rds-data:BatchExecuteStatement",
        "rds-data:BeginTransaction",
        "rds-data:CommitTransaction",
        "rds-data:RollbackTransaction",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetRandomPassword",
        "tag:GetResources"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSDirectoryServiceAccess

AmazonRDSDirectoryServiceAccess es una [política administrada por AWS](#) que permite a RDS acceder a Directory Service Managed AD en nombre del cliente para las instancias de base de datos de SQL Server incorporadas a un dominio.

Uso de esta política

Puede asociar AmazonRDSDirectoryServiceAccess a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio

- Hora de creación: 26 de febrero de 2016 a las 2:02 UTC
- Hora de edición: 15 de mayo de 2019 a las 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSEnhancedMonitoringRole

AmazonRDSEnhancedMonitoringRole es una [política administrada por AWS](#) que: proporciona acceso a Cloudwatch para Supervisión mejorada de RDS

Uso de esta política

Puede asociar AmazonRDSEnhancedMonitoringRole a los usuarios, grupos y roles.

Detalles de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de noviembre de 2015 a las 19:58 UTC
- Hora de edición: 11 de noviembre de 2015 a las 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    }
  ],
}
```

```
{
  "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSFullAccess

AmazonRDSFullAccess es una [AWS política administrada](#) que: brinda acceso total a Amazon RDS a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonRDSFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 17 de agosto de 2023 a las 23:00 UTC

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

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```

    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:GetCoipPoolUsage",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "sns:Publish",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "outposts:GetOutpostInstanceTypes",
    "devops-guru:GetResourceCollection"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "pi:*",
  "Resource" : [
    "arn:aws:pi:*:*:metrics/rds/*",
    "arn:aws:pi:*:*:perf-reports/rds/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [
        "rds.amazonaws.com",
        "rds.application-autoscaling.amazonaws.com"
      ]
    }
  }
},
{
  "Action" : [
    "devops-guru:SearchInsights",
    "devops-guru:ListAnomaliesForInsight"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "devops-guru:ServiceNames" : [

```

```
        "RDS"
      ]
    },
    "Null" : {
      "devops-guru:ServiceNames" : "false"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSPerformanceInsightsFullAccess

AmazonRDSPerformanceInsightsFullAccess es una [política administrada por AWS](#) que brinda acceso completo a RDS Performance Insights a través de la AWS Management Console

Uso de la política

Puede asociar AmazonRDSPerformanceInsightsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de agosto de 2023 a las 23:41 UTC
- Hora de edición: 23 de octubre de 2023 a las 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "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" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSPerformanceInsightsReadOnly

AmazonRDSPerformanceInsightsReadOnly es una [política administrada por AWS](#) que: es una política de solo lectura para RDS Performance Insights

Uso de la política

Puede asociar AmazonRDSPerformanceInsightsReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de abril de 2022 a las 00:02 UTC
- Hora de edición: 23 de octubre de 2023 a las 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
```

```

    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
    "Effect" : "Allow",
    "Action" : "pi:GetDimensionKeyDetails",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
    "Effect" : "Allow",
    "Action" : "pi:GetResourceMetadata",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
    "Effect" : "Allow",
    "Action" : "pi:GetResourceMetrics",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
    "Effect" : "Allow",
    "Action" : "pi:ListAvailableResourceDimensions",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
    "Effect" : "Allow",
    "Action" : "pi:ListAvailableResourceMetrics",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
    "Effect" : "Allow",
    "Action" : "pi:GetPerformanceAnalysisReport",
    "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
    "Effect" : "Allow",
    "Action" : "pi:ListPerformanceAnalysisReports",
    "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
  },
}

```

```
{
  "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
  "Effect" : "Allow",
  "Action" : "pi:ListTagsForResource",
  "Resource" : "arn:aws:pi:*:*:*/*/rds/*"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSPreviewServiceRolePolicy

AmazonRDSPreviewServiceRolePolicy es una [política administrada por AWS](#) que: es una política de rol de servicio de Amazon RDS Preview

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 31 de mayo de 2018 a las 18:02 UTC
- Hora de edición: 4 de octubre de 2023 a las 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteCoipPoolPermission",
        "ec2>DeleteLocalGatewayRouteTablePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",

```

```

    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DisassociateAddress",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "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"
    }
  }
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSReadOnlyAccess

AmazonRDSReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Amazon RDS a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonRDSReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 14 de abril de 2023 a las 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",

```

```
    "devops-guru:ListAnomaliesForInsight"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "devops-guru:ServiceNames" : [
        "RDS"
      ]
    },
    "Null" : {
      "devops-guru:ServiceNames" : "false"
    }
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRDSServiceRolePolicy

AmazonRDSServiceRolePolicy es una [política administrada por AWS](#) que: permite a Amazon RDS gestionar los recursos AWS por usted.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de enero de 2018 a las 18:17 UTC
- Hora editada: 19 de enero de 2024, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Versión de la política

Versión de la política: v13 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossRegionCommunication",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteCoipPoolPermission",
```

```

    "ec2:DeleteLocalGatewayRouteTablePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteSecurityGroup",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCoipPools",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTablePermissions",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DisassociateAddress",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifyVpcEndpoint",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeVpcEndpoints",
    "ec2>DeleteVpcEndpoints",
    "ec2:AssignPrivateIpAddresses",
    "ec2:UnassignPrivateIpAddresses"
  ],
  "Resource" : "*"
},
{
  "Sid" : "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"
    }
  }
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRedshiftAllCommandsFullAccess

AmazonRedshiftAllCommandsFullAccess es una [política administrada por AWS](#) que: incluye permisos para ejecutar comandos SQL para copiar, cargar, descargar, consultar y analizar datos en Amazon Redshift. La política también concede permisos para ejecutar instrucciones Select para servicios relacionados, como Amazon S3, los Registros de Amazon CloudWatch, Amazon SageMaker o AWS Glue.

Uso de la política

Puede asociar AmazonRedshiftAllCommandsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de noviembre de 2021 a las 00:48 UTC
- Hora de edición: 25 de noviembre de 2021 a las 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "SageMaker",
          "/aws/sagemaker/Endpoints",
          "/aws/sagemaker/ProcessingJobs",
          "/aws/sagemaker/TrainingJobs",
          "/aws/sagemaker/TransformJobs"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:BatchCheckLayerAvailability",
      "ecr:BatchGetImage",
      "ecr:GetAuthorizationToken",
      "ecr:GetDownloadUrlForLayer"
    ],
    "Resource" : "*"
  }
}

```

```

},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetEncryptionConfiguration",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:ListMultipartUploadParts",
    "s3:ListBucketMultipartUploads",
    "s3:PutObject",
    "s3:PutBucketAcl",
    "s3:PutBucketCors",
    "s3>DeleteObject",
    "s3:AbortMultipartUpload",
    "s3>CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::redshift-downloads",
    "arn:aws:s3:::redshift-downloads/*",
    "arn:aws:s3::*redshift*",
    "arn:aws:s3::*redshift/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/Redshift" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:Scan",
    "dynamodb:DescribeTable",

```

```
    "dynamodb:Getitem"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/*redshift*",
    "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticmapreduce:ListInstances"
  ],
  "Resource" : [
    "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticmapreduce:ListInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "elasticmapreduce:ResourceTag/Redshift" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:*redshift*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:UpdateDatabase",
    "glue:CreateTable",
```

```

    "glue:DeleteTable",
    "glue:BatchDeleteTable",
    "glue:UpdateTable",
    "glue:GetTable",
    "glue:GetTables",
    "glue:BatchCreatePartition",
    "glue:CreatePartition",
    "glue>DeletePartition",
    "glue:BatchDeletePartition",
    "glue:UpdatePartition",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchGetPartition"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/*redshift*/*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*redshift*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetResourcePolicy",
    "secretsmanager:GetSecretValue",
    "secretsmanager:DescribeSecret",
    "secretsmanager:ListSecretVersionIds"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:*redshift*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ]
}

```



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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRedshiftDataFullAccess

AmazonRedshiftDataFullAccess es una [política administrada por AWS](#) que: brinda acceso total a las API de datos de Amazon Redshift. Esta política también concede acceso definido a otros servicios requeridos.

Uso de la política

Puede asociar AmazonRedshiftDataFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de septiembre de 2020 a las 19:23 UTC

- Hora de edición: 7 de abril de 2023 a las 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
```

```

        "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
    }
}
},
{
    "Sid" : "GetCredentialsForAPIUser",
    "Effect" : "Allow",
    "Action" : "redshift:GetClusterCredentials",
    "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
    ]
},
{
    "Sid" : "GetCredentialsWithFederatedIAMCredentials",
    "Effect" : "Allow",
    "Action" : "redshift:GetClusterCredentialsWithIAM",
    "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
},
{
    "Sid" : "GetCredentialsForServerless",
    "Effect" : "Allow",
    "Action" : "redshift-serverless:GetCredentials",
    "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/RedshiftDataFullAccess" : "*"
        }
    }
},
{
    "Sid" : "DenyCreateAPIUser",
    "Effect" : "Deny",
    "Action" : "redshift:CreateClusterUser",
    "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
    ]
},
{
    "Sid" : "ServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/redshift-data.amazonaws.com/AWSServiceRoleForRedshift",

```

```
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "redshift-data.amazonaws.com"
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRedshiftFullAccess

AmazonRedshiftFullAccess es una [política administrada por AWS](#) que: brinda acceso total a Amazon Redshift a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonRedshiftFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 7 de julio de 2022 a las 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/AWSServiceRoleForRedshift",
    }
  ]
}
```

```

    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "redshift.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "DataAPIPermissions",
    "Action" : [
      "redshift-data:ExecuteStatement",
      "redshift-data:CancelStatement",
      "redshift-data:ListStatements",
      "redshift-data:GetStatementResult",
      "redshift-data:DescribeStatement",
      "redshift-data:ListDatabases",
      "redshift-data:ListSchemas",
      "redshift-data:ListTables",
      "redshift-data:DescribeTable"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerListPermissions",
    "Action" : [
      "secretsmanager:ListSecrets"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerCreateGetPermissions",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:TagResource"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
      }
    }
  }
}

```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRedshiftQueryEditor

AmazonRedshiftQueryEditor es una [política administrada por AWS](#) que: concede acceso total al Amazon Redshift Query Editor y a las consultas guardadas a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonRedshiftQueryEditor a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de octubre de 2018 a las 22:50 UTC
- Hora de edición: 16 de febrero de 2021 a las 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
        "redshift:DescribeSavedQueries",
        "redshift:CreateSavedQuery",
        "redshift>DeleteSavedQueries",
        "redshift:ModifySavedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIIAMSessionPermissionsRestriction",
      "Action" : [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",

```



```

    "redshift-data:DescribeStatement",
    "redshift-data:ListStatements"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "SecretsManagerListPermissions",
  "Action" : [
    "secretsmanager:ListSecrets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "SecretsManagerCreateGetPermissions",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:TagResource"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
  "Condition" : {
    "StringEquals" : {
      "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRedshiftQueryEditorV2FullAccess

AmazonRedshiftQueryEditorV2FullAccess es una [política administrada por AWS](#) que: concede acceso completo a todos los recursos y las operaciones del Amazon Redshift Query Editor V2. Esta política también concede acceso a otros servicios requeridos. Esto incluye permisos para enumerar los clústeres de Amazon Redshift, leer claves y alias en AWS KMS y administrar los secretos del Query Editor V2 en Secrets Manager AWS .

Uso de la política

Puede asociar AmazonRedshiftQueryEditorV2FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 24 de septiembre de 2021 a las 14:06 UTC
- Hora editada: 21 de febrero de 2024 a las 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusters",
      "redshift-serverless:ListNamespaces",
      "redshift-serverless:ListWorkgroups"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KeyManagementServicePermissions",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager>DeleteSecret",
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
  },
  {
    "Sid" : "ResourceGroupsTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
    "Effect" : "Allow",

```

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

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonRedshiftQueryEditorV2NoSharing

AmazonRedshiftQueryEditorV2NoSharing es una [política administrada por AWS](#) que: permite trabajar con el Amazon Redshift Query Editor V2 sin compartir recursos. La entidad principal autorizada solo puede leer, actualizar y eliminar sus propios recursos, pero no puede compartirlos. Esta política también concede acceso a otros servicios requeridos. Esto incluye permisos para enumerar los clústeres de Amazon Redshift y administrar los secretos del editor de consultas V2 del director en AWS Secrets Manager.

Uso de la política

Puede asociar AmazonRedshiftQueryEditorV2NoSharing a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 24 de septiembre de 2021 a las 14:18 UTC
- Hora editada: 21 de febrero de 2024 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```

    "tag:GetResources"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateFolder",
    "sqlworkbench:PutTab",
    "sqlworkbench:BatchDeleteFolder",
    "sqlworkbench>DeleteTab",
    "sqlworkbench:GenerateSession",
    "sqlworkbench:GetAccountInfo",
    "sqlworkbench:GetAccountSettings",
    "sqlworkbench:GetUserInfo",
    "sqlworkbench:GetUserWorkspaceSettings",
    "sqlworkbench:PutUserWorkspaceSettings",
    "sqlworkbench>ListConnections",
    "sqlworkbench>ListFiles",
    "sqlworkbench>ListTabs",
    "sqlworkbench:UpdateFolder",
    "sqlworkbench>ListRedshiftClusters",
    "sqlworkbench:DriverExecute",
    "sqlworkbench>ListTaggedResources",
    "sqlworkbench>ListQueryExecutionHistory",
    "sqlworkbench:GetQueryExecutionHistory",
    "sqlworkbench>ListNotebooks",
    "sqlworkbench:GetSchemaInference",
    "sqlworkbench:GetAutocompletionMetadata",
    "sqlworkbench:GetAutocompletionResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench>CreateConnection",

```

```

    "sqlworkbench:CreateSavedQuery",
    "sqlworkbench:CreateChart",
    "sqlworkbench:CreateNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws: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}"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonRedshiftQueryEditorV2ReadSharing

AmazonRedshiftQueryEditorV2ReadSharing es una [política administrada por AWS](#) que: permite trabajar con el Amazon Redshift Query Editor V2 con capacidad limitada para compartir recursos. La entidad principal concedida puede leer, escribir y compartir sus propios recursos. La entidad principal concedida puede leer los recursos compartidos con su equipo, pero no puede actualizarlos. Esta política también concede acceso a otros servicios requeridos. Esto incluye permisos para enumerar los clústeres de Amazon Redshift y administrar los secretos del editor de consultas V2 del director en AWS Secrets Manager.

Uso de la política

Puede asociar AmazonRedshiftQueryEditorV2ReadSharing a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de septiembre de 2021 a las 14:22 UTC
- Hora editada: 21 de febrero de 2024 a las 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```

    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecretsManagerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
  "Condition" : {
    "StringEquals" : {
      "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "ResourceGroupsTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateFolder",
    "sqlworkbench:PutTab",
    "sqlworkbench:BatchDeleteFolder",
    "sqlworkbench>DeleteTab",
    "sqlworkbench:GenerateSession",
    "sqlworkbench:GetAccountInfo",

```

```

    "sqlworkbench:GetAccountSettings",
    "sqlworkbench:GetUserInfo",
    "sqlworkbench:GetUserWorkspaceSettings",
    "sqlworkbench:PutUserWorkspaceSettings",
    "sqlworkbench:ListConnections",
    "sqlworkbench:ListFiles",
    "sqlworkbench:ListTabs",
    "sqlworkbench:UpdateFolder",
    "sqlworkbench:ListRedshiftClusters",
    "sqlworkbench:DriverExecute",
    "sqlworkbench:ListTaggedResources",
    "sqlworkbench:ListQueryExecutionHistory",
    "sqlworkbench:GetQueryExecutionHistory",
    "sqlworkbench:ListNotebooks",
    "sqlworkbench:GetSchemaInference",
    "sqlworkbench:GetAutocompletionMetadata",
    "sqlworkbench:GetAutocompletionResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateConnection",
    "sqlworkbench:CreateSavedQuery",
    "sqlworkbench:CreateChart",
    "sqlworkbench:CreateNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench>DeleteChart",

```

```

    "sqlworkbench:DeleteConnection",
    "sqlworkbench:DeleteSavedQuery",
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:UpdateFileFolder",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:UpdateNotebook",
    "sqlworkbench>DeleteNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench>CreateNotebookCell",
    "sqlworkbench>DeleteNotebookCell",
    "sqlworkbench:UpdateNotebookCellContent",
    "sqlworkbench:UpdateNotebookCellLayout",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench>CreateNotebookVersion",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench>DeleteNotebookVersion",
    "sqlworkbench:RestoreNotebookVersion",
    "sqlworkbench>CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",

```

```

"Resource" : "*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : "sqlworkbench-resource-owner"
  },
  "StringEquals" : {
    "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
    "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
  }
}
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench>CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {

```

```

    "aws:TagKeys" : "sqlworkbench-team"
  },
  "StringEquals" : {
    "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
    "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
  }
}
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:UntagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-team"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

AmazonRedshiftQueryEditorV2ReadWriteSharing es una [política administrada por AWS](#) que: permite trabajar con el Amazon Redshift Query Editor V2 con capacidad para compartir recursos. La entidad principal concedida puede leer, escribir y compartir sus propios recursos. La entidad principal concedida puede leer y actualizar los recursos compartidos con su equipo. Esta

política también concede acceso a otros servicios requeridos. Esto incluye permisos para enumerar los clústeres de Amazon Redshift y administrar los secretos del editor de consultas V2 del director en AWS Secrets Manager.

Uso de la política

Puede asociar `AmazonRedshiftQueryEditorV2ReadWriteSharing` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 24 de septiembre de 2021 a las 14:25 UTC
- Hora editada: 21 de febrero de 2024 a las 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
```

```

    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager>DeleteSecret",
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
    "Condition" : {
      "StringEquals" : {
        "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
      }
    }
  },
  {
    "Sid" : "ResourceGroupsTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateFolder",
      "sqlworkbench:PutTab",
      "sqlworkbench:BatchDeleteFolder",
      "sqlworkbench>DeleteTab",
      "sqlworkbench:GenerateSession",
      "sqlworkbench:GetAccountInfo",
      "sqlworkbench:GetAccountSettings",
      "sqlworkbench:GetUserInfo",
      "sqlworkbench:GetUserWorkspaceSettings",
      "sqlworkbench:PutUserWorkspaceSettings",
      "sqlworkbench>ListConnections",
      "sqlworkbench>ListFiles",

```



```

    "sqlworkbench:ListTabs",
    "sqlworkbench:UpdateFolder",
    "sqlworkbench:ListRedshiftClusters",
    "sqlworkbench:DriverExecute",
    "sqlworkbench:ListTaggedResources",
    "sqlworkbench:ListQueryExecutionHistory",
    "sqlworkbench:GetQueryExecutionHistory",
    "sqlworkbench:ListNotebooks",
    "sqlworkbench:GetSchemaInference",
    "sqlworkbench:GetAutocompletionMetadata",
    "sqlworkbench:GetAutocompletionResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateConnection",
    "sqlworkbench:CreateSavedQuery",
    "sqlworkbench:CreateChart",
    "sqlworkbench:CreateNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws: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" : "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}"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonRedshiftReadOnlyAccess

AmazonRedshiftReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a Amazon Redshift a través del. AWS Management Console

Uso de la política

Puede asociar `AmazonRedshiftReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 8 de febrero de 2024 a las 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftReadOnlyAccess",
      "Action" : [
        "redshift:Describe*",
        "redshift:ListRecommendations",
        "redshift:ViewQueriesInConsole",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:Get*",
        "sns:List*",

```

```
        "cloudwatch:Describe*",
        "cloudwatch:List*",
        "cloudwatch:Get*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonRedshiftServiceLinkedRolePolicy

AmazonRedshiftServiceLinkedRolePolicy es una [política AWS gestionada](#) que: permite a Amazon Redshift llamar a los AWS servicios en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de septiembre de 2017 a las 19:19 UTC
- Hora editada: 15 de marzo de 2024 a las 20:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v13 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2>CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
```

```

    "StringEquals" : {
      "aws:RequestTag/Redshift" : "true"
    }
  },
  {
    "Sid" : "PublicAccessReleaseEip",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ReleaseAddress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:elastic-ip/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/Redshift" : "true"
      }
    }
  },
  {
    "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:PutRetentionPolicy"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/redshift/*"
    ]
  },
  {
    "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
    ]
  },

```



```
{
  "Sid" : "CreateSecurityGroupWithTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Redshift" : "true"
    }
  }
},
{
  "Sid" : "SecurityGroupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:ModifySecurityGroupRules",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/Redshift" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroup",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*"
  ]
}
```

```

},
{
  "Sid" : "CreateTagsOnResources",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:internet-gateway/*",
    "arn:aws:ec2:*:*:elastic-ip/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateVpc",
        "CreateSecurityGroup",
        "CreateSubnet",
        "CreateInternetGateway",
        "CreateRouteTable",
        "AllocateAddress"
      ]
    }
  }
},
{
  "Sid" : "VPCPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSecurityGroupRules",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatch",
  "Effect" : "Allow",
  "Action" : [

```

```

    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/Redshift-Serverless",
        "AWS/Redshift"
      ]
    }
  }
},
{
  "Sid" : "SecretManager",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:PutSecretValue",
    "secretsmanager:UpdateSecret",
    "secretsmanager:UpdateSecretVersionStage",
    "secretsmanager:RotateSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:redshift!*"
  ],
  "Condition" : {
    "StringEquals" : {
      "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "SecretsManagerRandomPassword",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IPV6Permissions",
  "Effect" : "Allow",

```

```
    "Action" : [
      "ec2:AssignIpv6Addresses",
      "ec2:UnassignIpv6Addresses"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ]
  },
  {
    "Sid" : "ServiceQuotasToCheckCustomerLimits",
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:GetServiceQuota"
    ],
    "Resource" : [
      "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
      "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonRekognitionCustomLabelsFullAccess

AmazonRekognitionCustomLabelsFullAccess es una [política administrada por AWS](#) que especifica los permisos de reconocimiento y s3 que requiere la característica de etiquetas personalizadas de Amazon Rekognition.

Uso de la política

Puede asociar AmazonRekognitionCustomLabelsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de enero de 2020 a las 19:18 UTC
- Hora de edición: 16 de agosto de 2022 a las 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3::*custom-labels*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CreateProject",
        "rekognition:CreateProjectVersion",
```

```

    "rekognition:StartProjectVersion",
    "rekognition:StopProjectVersion",
    "rekognition:DescribeProjects",
    "rekognition:DescribeProjectVersions",
    "rekognition:DetectCustomLabels",
    "rekognition>DeleteProject",
    "rekognition>DeleteProjectVersion",
    "rekognition:TagResource",
    "rekognition:UntagResource",
    "rekognition:ListTagsForResource",
    "rekognition>CreateDataset",
    "rekognition:ListDatasetEntries",
    "rekognition:ListDatasetLabels",
    "rekognition:DescribeDataset",
    "rekognition:UpdateDatasetEntries",
    "rekognition:DistributeDatasetEntries",
    "rekognition>DeleteDataset",
    "rekognition:CopyProjectVersion",
    "rekognition:PutProjectPolicy",
    "rekognition:ListProjectPolicies",
    "rekognition>DeleteProjectPolicy"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRekognitionFullAccess

AmazonRekognitionFullAccess es una [política administrada por AWS](#) que: concede acceso a todas las API de Amazon Rekognition

Uso de la política

Puede asociar AmazonRekognitionFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2016 a las 14:40 UTC
- Hora de edición: 30 de noviembre de 2016 a las 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRekognitionReadOnlyAccess

AmazonRekognitionReadOnlyAccess es una [política administrada por AWS](#) que: accede a todas las API de reconocimiento de lectura

Uso de la política

Puede asociar AmazonRekognitionReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2016 a las 14:58 UTC
- Hora de edición: 8 de noviembre de 2023 a las 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
    "rekognition:DetectFaces",
    "rekognition:DetectLabels",
    "rekognition:ListCollections",
    "rekognition:ListFaces",
    "rekognition:SearchFaces",
    "rekognition:SearchFacesByImage",
    "rekognition:DetectText",
    "rekognition:GetCelebrityInfo",
    "rekognition:RecognizeCelebrities",
    "rekognition:DetectModerationLabels",
    "rekognition:GetLabelDetection",
    "rekognition:GetFaceDetection",
    "rekognition:GetContentModeration",
    "rekognition:GetPersonTracking",
    "rekognition:GetCelebrityRecognition",
    "rekognition:GetFaceSearch",
    "rekognition:GetTextDetection",
    "rekognition:GetSegmentDetection",
    "rekognition:DescribeStreamProcessor",
    "rekognition:ListStreamProcessors",
    "rekognition:DescribeProjects",
    "rekognition:DescribeProjectVersions",
    "rekognition:DetectCustomLabels",
    "rekognition:DetectProtectiveEquipment",
    "rekognition:ListTagsForResource",
    "rekognition:ListDatasetEntries",
    "rekognition:ListDatasetLabels",
    "rekognition:DescribeDataset",
    "rekognition:ListProjectPolicies",
    "rekognition:ListUsers",
    "rekognition:SearchUsers",
    "rekognition:SearchUsersByImage",
    "rekognition:GetMediaAnalysisJob",
    "rekognition:ListMediaAnalysisJobs"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRekognitionServiceRole

AmazonRekognitionServiceRole es una [política administrada por AWS](#) que: permite a Rekognition llamar a los servicios de AWS en su nombre.

Uso de la política

Puede asociar AmazonRekognitionServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de noviembre de 2017 a las 16:52 UTC
- Hora de edición: 29 de noviembre de 2017 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:PutRecord",
      "kinesis:PutRecords"
    ],
    "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:GetDataEndpoint",
      "kinesisvideo:GetMedia"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53AutoNamingFullAccess

AmazonRoute53AutoNamingFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todas las acciones de denominación automática de Route 53.

Uso de la política

Puede asociar `AmazonRoute53AutoNamingFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de enero de 2018 a las 18:40 UTC
- Hora de edición: 18 de enero de 2018 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53>DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "servicediscovery:*"
      ]
    }
  ]
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53AutoNamingReadOnlyAccess

AmazonRoute53AutoNamingReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a todas las acciones de denominación automática de Route 53.

Uso de la política

Puede asociar AmazonRoute53AutoNamingReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de enero de 2018 a las 03:02 UTC
- Hora de edición: 18 de enero de 2018 a las 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53AutoNamingRegistrantAccess

AmazonRoute53AutoNamingRegistrantAccess es una [política administrada por AWS](#) que brinda acceso a nivel de registrante a las acciones de denominación automática de Route 53.

Uso de la política

Puede asociar AmazonRoute53AutoNamingRegistrantAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de marzo de 2018 a las 22:33 UTC
- Hora de edición: 12 de marzo de 2018 a las 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53DomainsFullAccess

AmazonRoute53DomainsFullAccess es una [política administrada por AWS](#) que: concede acceso total a todas las acciones de Route53 Domains, y crea una Zona alojada para permitir la creación de zonas alojadas como parte de los registros de dominio.

Uso de la política

Puede asociar AmazonRoute53DomainsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53DomainsReadOnlyAccess

AmazonRoute53DomainsReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso a la lista y las acciones de los dominios de Route53.

Uso de la política

Puede asociar AmazonRoute53DomainsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53FullAccess

AmazonRoute53FullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todos los Amazon Route 53 a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonRoute53FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 20 de diciembre de 2018 a las 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53ReadOnlyAccess

AmazonRoute53ReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a todos los Amazon Route 53 a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonRoute53ReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 15 de noviembre de 2016 a las 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53RecoveryClusterFullAccess

AmazonRoute53RecoveryClusterFullAccess es una [política administrada por AWS](#) que: concede acceso completo al clúster de recuperación de Amazon Route 53

Uso de la política

Puede asociar AmazonRoute53RecoveryClusterFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de agosto de 2021 a las 18:37 UTC
- Hora de edición: 18 de agosto de 2021 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

AmazonRoute53RecoveryClusterReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura al clúster de recuperación de Amazon Route 53

Uso de la política

Puede asociar AmazonRoute53RecoveryClusterReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de agosto de 2021 a las 17:36 UTC
- Hora de edición: 1 de abril de 2022 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "route53-recovery-cluster:GetRoutingControlState",
      "route53-recovery-cluster:ListRoutingControls"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53RecoveryControlConfigFullAccess

AmazonRoute53RecoveryControlConfigFullAccess es una [política administrada por AWS](#) que: concede acceso total a Amazon Route 53 Recovery Control Config

Uso de la política

Puede asociar AmazonRoute53RecoveryControlConfigFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de agosto de 2021 a las 17:48 UTC
- Hora de edición: 18 de agosto de 2021 a las 17:48 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

`AmazonRoute53RecoveryControlConfigReadOnlyAccess` es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Route 53 Recovery Control Config

Uso de la política

Puede asociar `AmazonRoute53RecoveryControlConfigReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de agosto de 2021 a las 18:01 UTC
- Hora de edición: 18 de octubre de 2023 a las 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",

```

```
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53RecoveryReadinessFullAccess

AmazonRoute53RecoveryReadinessFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Route 53 Recovery Readiness

Uso de la política

Puede asociar AmazonRoute53RecoveryReadinessFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de agosto de 2021 a las 16:45 UTC
- Hora de edición: 18 de agosto de 2021 a las 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

AmazonRoute53RecoveryReadinessReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a Amazon Route 53 Recovery Readiness

Uso de la política

Puede asociar AmazonRoute53RecoveryReadinessReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de agosto de 2021 a las 18:11 UTC
- Hora de edición: 9 de noviembre de 2021 a las 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "route53-recovery-readiness:GetArchitectureRecommendations",
    "route53-recovery-readiness:GetCellReadinessSummary"
  ],
  "Resource" : "arn:aws:route53-recovery-readiness:*:*:*"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53ResolverFullAccess

AmazonRoute53ResolverFullAccess es una [política administrada por AWS](#) que: es una política de acceso total para Route 53 Resolver

Uso de la política

Puede asociar AmazonRoute53ResolverFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de mayo de 2019 a las 18:10 UTC
- Hora de edición: 17 de julio de 2020 a las 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonRoute53ResolverReadOnlyAccess

AmazonRoute53ResolverReadOnlyAccess es una [política administrada por AWS](#) que: es una política de solo lectura para Route 53 Resolver

Uso de la política

Puede asociar AmazonRoute53ResolverReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de mayo de 2019 a las 18:11 UTC
- Hora de edición: 27 de septiembre de 2019 a las 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",

```



```
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonS3FullAccess

AmazonS3FullAccess es una [política administrada por AWS](#) que: brinda acceso total a todos los depósitos a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonS3FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 27 de septiembre de 2021 a las 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonS3ObjectLambdaExecutionRolePolicy

AmazonS3ObjectLambdaExecutionRolePolicy es una [política administrada por AWS](#) que concede permisos a las funciones de Lambda de AWS para interactuar con Amazon S3 Object Lambda. También, concede permisos a Lambda para escribir en los Registros de CloudWatch.

Uso de la política

Puede asociar `AmazonS3ObjectLambdaExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de agosto de 2021 a las 10:07 UTC
- Hora de edición: 18 de agosto de 2021 a las 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonS3OutpostsFullAccess

AmazonS3OutpostsFullAccess es una [política administrada por AWS](#) que: otorga acceso total a Amazon S3 en Outposts a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonS3OutpostsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de octubre de 2020 a las 17:26 UTC
- Hora de edición: 2 de octubre de 2020 a las 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "s3-outposts:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "datasync:ListTasks",
      "datasync:ListLocations",
      "datasync:DescribeTask",
      "datasync:DescribeLocation*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "outposts:ListOutposts",
      "outposts:GetOutpost"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonS3OutpostsReadOnlyAccess

AmazonS3OutpostsReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a Amazon S3 en Outposts a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonS3OutpostsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de octubre de 2020 a las 18:55 UTC
- Hora de edición: 2 de octubre de 2020 a las 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "s3-outposts:Get*",
        "s3-outposts:List*"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
    ],
    "Resource" : "*"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonS3ReadOnlyAccess

AmazonS3ReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a todos los depósitos a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonS3ReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 10 de agosto de 2023 a las 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",

```



```
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy es una [política administrada por AWS](#) que: es una política de rol de servicio utilizada por el servicio de catálogo de Servicio de AWS para aprovisionar los productos de la cartera de Amazon SageMaker. Otorga permisos a un conjunto de servicios relacionados, incluidos CodePipeline, CodeBuild, CodeCommit, Glue, CloudFormation, etc.

Uso de la política

Puede asociar AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2020 a las 18:48 UTC
- Hora de edición: 2 de agosto de 2022 a las 19:12 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerCanvasAIServiceAccess

AmazonSageMakerCanvasAIServiceAccesses una [política AWS gestionada](#) que: proporciona permisos para que Amazon SageMaker Canvas utilice los servicios de IA a fin de respaldar soluciones de IA listas para usar. Esta política añadirá más permisos de mutación para los servicios a medida que Amazon SageMaker Canvas vaya añadiendo compatibilidad.

Uso de la política

Puede asociar AmazonSageMakerCanvasAIServiceAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de marzo de 2023 a las 22:36 UTC
- Hora editada: 29 de noviembre de 2023 a las 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServiceAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
        "textract:StartDocumentAnalysis",
        "textract:StartExpenseAnalysis",
        "textract:GetDocumentAnalysis",
        "textract:GetExpenseAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Rekognition",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectLabels",
        "rekognition:DetectText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Comprehend",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:BatchDetectEntities",
        "comprehend:BatchDetectSentiment",
```

```

    "comprehend:DetectPiiEntities",
    "comprehend:DetectEntities",
    "comprehend:DetectSentiment",
    "comprehend:DetectDominantLanguage"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Bedrock",
  "Effect" : "Allow",
  "Action" : [
    "bedrock:InvokeModel",
    "bedrock:ListFoundationModels",
    "bedrock:InvokeModelWithResponseStream"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateBedrockResourcesPermission",
  "Effect" : "Allow",
  "Action" : [
    "bedrock:CreateModelCustomizationJob",
    "bedrock:CreateProvisionedModelThroughput",
    "bedrock:TagResource"
  ],
  "Resource" : [
    "arn:aws:bedrock:*:*:model-customization-job/*",
    "arn:aws:bedrock:*:*:custom-model/*",
    "arn:aws:bedrock:*:*:provisioned-model/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "SageMaker",
        "Canvas"
      ]
    }
  },
  "StringEquals" : {
    "aws:RequestTag/SageMaker" : "true",
    "aws:RequestTag/Canvas" : "true",
    "aws:ResourceTag/SageMaker" : "true",
    "aws:ResourceTag/Canvas" : "true"
  }
}
}

```

```
},
{
  "Sid" : "GetStopAndDeleteBedrockResourcesPermission",
  "Effect" : "Allow",
  "Action" : [
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetCustomModel",
    "bedrock:GetProvisionedModelThroughput",
    "bedrock:StopModelCustomizationJob",
    "bedrock>DeleteProvisionedModelThroughput"
  ],
  "Resource" : [
    "arn:aws:bedrock:*:*:model-customization-job/*",
    "arn:aws:bedrock:*:*:custom-model/*",
    "arn:aws:bedrock:*:*:provisioned-model/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SageMaker" : "true",
      "aws:ResourceTag/Canvas" : "true"
    }
  }
},
{
  "Sid" : "FoundationModelPermission",
  "Effect" : "Allow",
  "Action" : [
    "bedrock:CreateModelCustomizationJob"
  ],
  "Resource" : [
    "arn:aws:bedrock:*:*:foundation-model/*"
  ]
},
{
  "Sid" : "BedrockFineTuningPassRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/*"
  ],
  "Condition" : {
    "StringEquals" : {
```

```
        "iam:PassedToService" : "bedrock.amazonaws.com"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerCanvasBedrockAccess

AmazonSageMakerCanvasBedrockAccesses una [política AWS gestionada](#) que: esta política concede permisos para usar Amazon Bedrock in SageMaker Canvas al proporcionar acceso a servicios descendentes como S3.

Uso de la política

Puede asociar AmazonSageMakerCanvasBedrockAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de febrero de 2024 a las 18:37 UTC
- Hora editada: 2 de febrero de 2024 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas",
        "arn:aws:s3:::sagemaker-*/Canvas/*"
      ]
    },
    {
      "Sid" : "S3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerCanvasDataPrepFullAccess

AmazonSageMakerCanvasDataPrepFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a SageMaker los recursos y operaciones de Amazon para la preparación de datos en Canvas. La política también proporciona acceso selecto a servicios relacionados (por ejemplo, S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena EventBridge, Glue o Secrets Manager). Esta política debe adjuntarse a la función de ejecución del SageMaker dominio o perfil de usuario de Amazon.

Uso de la política

Puede asociar AmazonSageMakerCanvasDataPrepFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de octubre de 2023 a las 22:56 UTC
- Hora editada: 8 de diciembre de 2023 a las 02:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Effect" : "Allow",
    "Action" : "sagemaker:ListFeatureGroups",
    "Resource" : "*"
  },
  {
    "Sid" : "SageMakerFeatureGroupOperations",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateFeatureGroup",
      "sagemaker:DescribeFeatureGroup"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
  },
  {
    "Sid" : "SageMakerProcessingJobOperations",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateProcessingJob",
      "sagemaker:DescribeProcessingJob",
      "sagemaker:AddTags"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
  },
  {
    "Sid" : "SageMakerProcessingJobListOperation",
    "Effect" : "Allow",
    "Action" : "sagemaker:ListProcessingJobs",
    "Resource" : "*"
  },
  {
    "Sid" : "SageMakerPipelineOperations",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:DescribePipeline",
      "sagemaker:CreatePipeline",
      "sagemaker:UpdatePipeline",
      "sagemaker>DeletePipeline",
      "sagemaker:StartPipelineExecution",
      "sagemaker:ListPipelineExecutionSteps",
      "sagemaker:DescribePipelineExecution"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
  },
  {

```

```

    "Sid" : "KMSListOperations",
    "Effect" : "Allow",
    "Action" : "kms:ListAliases",
    "Resource" : "*"
  },
  {
    "Sid" : "KMSOperations",
    "Effect" : "Allow",
    "Action" : "kms:DescribeKey",
    "Resource" : "arn:aws:kms:*:*:key/*"
  },
  {
    "Sid" : "S3Operations",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:GetBucketCors",
      "s3:GetBucketLocation",
      "s3:AbortMultipartUpload"
    ],
    "Resource" : [
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "S3GetObjectOperation",
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "arn:aws:s3::*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/SageMaker" : "true"
      },
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }

```

```

    }
  }
},
{
  "Sid" : "S3ListOperations",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMListOperations",
  "Effect" : "Allow",
  "Action" : "iam:ListRoles",
  "Resource" : "*"
},
{
  "Sid" : "IAMGetOperations",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/*"
},
{
  "Sid" : "IAMPassOperation",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com",
        "events.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "EventBridgePutOperation",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
  ],

```

```

    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
      }
    }
  },
  {
    "Sid" : "EventBridgeOperations",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:PutTargets"
    ],
    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
      }
    }
  },
  {
    "Sid" : "EventBridgeTagBasedOperations",
    "Effect" : "Allow",
    "Action" : [
      "events:TagResource"
    ],
    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
        "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
      }
    }
  },
  {
    "Sid" : "EventBridgeListTagOperation",
    "Effect" : "Allow",
    "Action" : "events:ListTagsForResource",
    "Resource" : "*"
  },
  {
    "Sid" : "GlueOperations",
    "Effect" : "Allow",

```

```

    "Action" : [
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables",
      "glue:SearchTables"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:table/*",
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/*"
    ]
  },
  {
    "Sid" : "EMROperations",
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:DescribeCluster",
      "elasticmapreduce:ListInstanceGroups"
    ],
    "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
  },
  {
    "Sid" : "EMRListOperation",
    "Effect" : "Allow",
    "Action" : "elasticmapreduce:ListClusters",
    "Resource" : "*"
  },
  {
    "Sid" : "AthenaListDataCatalogOperation",
    "Effect" : "Allow",
    "Action" : "athena:ListDataCatalogs",
    "Resource" : "*"
  },
  {
    "Sid" : "AthenaQueryExecutionOperations",
    "Effect" : "Allow",
    "Action" : [
      "athena:GetQueryExecution",
      "athena:GetQueryResults",
      "athena:StartQueryExecution",
      "athena:StopQueryExecution"
    ],
    "Resource" : "arn:aws:athena:*:*:workgroup/*"
  },
}

```

```

{
  "Sid" : "AthenaDataCatalogOperations",
  "Effect" : "Allow",
  "Action" : [
    "athena:ListDatabases",
    "athena:ListTableMetadata"
  ],
  "Resource" : "arn:aws:athena:*:*:datacatalog/*"
},
{
  "Sid" : "RedshiftOperations",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:DescribeStatement",
    "redshift-data:CancelStatement",
    "redshift-data:GetStatementResult"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RedshiftArnBasedOperations",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables"
  ],
  "Resource" : "arn:aws:redshift:*:*:cluster:*"
},
{
  "Sid" : "RedshiftGetCredentialsOperation",
  "Effect" : "Allow",
  "Action" : "redshift:GetClusterCredentials",
  "Resource" : [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
  ]
},
{
  "Sid" : "SecretsManagerARNBasedOperation",
  "Effect" : "Allow",
  "Action" : "secretsmanager:CreateSecret",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
},

```



```

{
  "Sid" : "SecretManagerTagBasedOperation",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SageMaker" : "true",
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "RDSOperation",
  "Effect" : "Allow",
  "Action" : "rds:DescribeDBInstances",
  "Resource" : "*"
},
{
  "Sid" : "LoggingOperation",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerCanvasDirectDeployAccess

AmazonSageMakerCanvasDirectDeployAccess es una [política administrada por AWS](#) que: permite que Amazon SageMaker Canvas cree, gestione y vea los detalles de los puntos de conexión creados a través de Canvas. Permite que Amazon SageMaker Canvas recupere las métricas de invocación de puntos de conexión de CloudWatch.

Uso de la política

Puede asociar AmazonSageMakerCanvasDirectDeployAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de octubre de 2023 a las 18:11 UTC
- Hora de edición: 6 de octubre de 2023 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Action" : [
      "sagemaker:CreateEndpoint",
      "sagemaker:CreateEndpointConfig",
      "sagemaker>DeleteEndpoint",
      "sagemaker:DescribeEndpoint",
      "sagemaker:DescribeEndpointConfig",
      "sagemaker:InvokeEndpoint",
      "sagemaker:UpdateEndpoint"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:Canvas*",
      "arn:aws:sagemaker:*:*:canvas*"
    ]
  },
  {
    "Sid" : "ReadCWInvocationMetrics",
    "Effect" : "Allow",
    "Action" : "cloudwatch:GetMetricData",
    "Resource" : "*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerCanvasForecastAccess

AmazonSageMakerCanvasForecastAccess es una [política administrada por AWS](#) que: concede los permisos que normalmente se necesitan para utilizar SageMaker Canvas con Amazon Forecast.

Uso de la política

Puede asociar AmazonSageMakerCanvasForecastAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de agosto de 2022 a las 20:04 UTC
- Hora de edición: 24 de agosto de 2022 a las 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

```
}  
 ]  
 }
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerCanvasFullAccess

AmazonSageMakerCanvasFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a los recursos y operaciones de Amazon SageMaker Canvas. La política también proporciona acceso selecto a servicios relacionados (por ejemplo, S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager y Forecast). Esta política debe adjuntarse a la función de ejecución del SageMaker dominio o perfil de usuario de Amazon.

Uso de la política

Puede asociar AmazonSageMakerCanvasFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de septiembre de 2022 a las 00:44 UTC
- Hora editada: 24 de enero de 2024 a las 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",

```

```

    "sagemaker:CreateModel",
    "sagemaker:CreateProcessingJob",
    "sagemaker:CreateAutoMLJob",
    "sagemaker:CreateAutoMLJobV2",
    "sagemaker>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"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerClusterInstanceRolePolicy

AmazonSageMakerClusterInstanceRolePolicy es una [política AWS gestionada](#) que: Esta política concede los permisos que normalmente se necesitan para usar Amazon SageMaker Cluster.

Uso de la política

Puede asociar AmazonSageMakerClusterInstanceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2023 a las 15:11 UTC
- Hora editada: 29 de noviembre de 2023 a las 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

"Statement" : [
  {
    "Sid" : "CloudwatchLogStreamPublishPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
    ]
  },
  {
    "Sid" : "CloudwatchLogGroupCreationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
    ]
  },
  {
    "Sid" : "CloudwatchPutMetricDataAccess",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
      }
    }
  },
  {
    "Sid" : "DataRetrievalFromS3BucketPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetObject"
    ]
  }
]

```

```
    ],
    "Resource" : [
      "arn:aws:s3:::sagemaker-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "SSMConnectivityPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssmmessages:CreateControlChannel",
      "ssmmessages:CreateDataChannel",
      "ssmmessages:OpenControlChannel",
      "ssmmessages:OpenDataChannel"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerCoreServiceRolePolicy

AmazonSageMakerCoreServiceRolePolicy es una [política administrada por AWS](#) para: el rol de servicio vinculado a un servicio para los servicios centrales de Amazon SageMaker

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de diciembre de 2020 a las 21:40 UTC
- Hora de edición: 21 de diciembre de 2020 a las 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
    }
  ]
}
```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerEdgeDeviceFleetPolicy

AmazonSageMakerEdgeDeviceFleetPolicy es una [política administrada por AWS](#) que proporciona los permisos que Sagemaker Edge necesita para crear y gestionar una flota de dispositivos para el cliente mediante la conexión a la nube predeterminada.

Uso de la política

Puede asociar AmazonSageMakerEdgeDeviceFleetPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 8 de diciembre de 2020 a las 16:17 UTC
- Hora de edición: 8 de diciembre de 2020 a las 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*",
        "arn:aws:s3::*Sagemaker*",
        "arn:aws:s3::*sagemaker*"
      ]
    },
    {
      "Sid" : "SageMakerEdgeApis",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SendHeartbeat",
        "sagemaker:GetDeviceRegistration"
      ],
      "Resource" : "*"
    }
  ],
  {
```

```

    "Sid" : "CreateIoTRoleAlias",
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateRoleAlias",
      "iot:DescribeRoleAlias",
      "iot:UpdateRoleAlias",
      "iot:ListTagsForResource",
      "iot:TagResource"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
    ]
  },
  {
    "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/*SageMaker*",
      "arn:aws:iam:*:*:role/*Sagemaker*",
      "arn:aws:iam:*:*:role/*sagemaker*"
    ]
  },
  {
    "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/*SageMaker*",
      "arn:aws:iam:*:*:role/*Sagemaker*",
      "arn:aws:iam:*:*:role/*sagemaker*"
    ],
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : [
          "iot.amazonaws.com",
          "credentials.iot.amazonaws.com"
        ]
      }
    }
  }
}

```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerFeatureStoreAccess

AmazonSageMakerFeatureStoreAccess es una [política administrada por AWS](#) que: otorga los permisos necesarios para habilitar la tienda sin conexión de un grupo de características de Amazon SageMaker FeatureStore.

Uso de la política

Puede asociar AmazonSageMakerFeatureStoreAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2020 a las 16:24 UTC
- Hora de edición: 5 de diciembre de 2022 a las 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*",
        "arn:aws:s3::*Sagemaker*",
        "arn:aws:s3::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*/metadata/*",
        "arn:aws:s3::*Sagemaker*/metadata/*",
        "arn:aws:s3::*sagemaker*/metadata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerFullAccess

AmazonSageMakerFullAccess es una [política AWS gestionada](#) que: proporciona acceso total a Amazon SageMaker a través del SDK AWS Management Console y. También proporciona acceso selecto a servicios relacionados (por ejemplo, S3, ECR, CloudWatch Logs).

Uso de la política

Puede asociar AmazonSageMakerFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2017 a las 13:07 UTC
- Hora editada: 30 de noviembre de 2023 a las 13:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Versión de la política

Versión de la política: v25 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AllowAllNonAdminSageMakerActions",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:*",
      "sagemaker-geospatial:*"
    ],
    "NotResource" : [
      "arn:aws:sagemaker:*:*:domain/*",
      "arn:aws:sagemaker:*:*:user-profile/*",
      "arn:aws:sagemaker:*:*:app/*",
      "arn:aws:sagemaker:*:*:space/*",
      "arn:aws:sagemaker:*:*:flow-definition/*"
    ]
  },
  {
    "Sid" : "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" : "*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerGeospatialExecutionRole

AmazonSageMakerGeospatialExecutionRole es una [política administrada por AWS](#) que brinda acceso a los servicios que se necesitan habitualmente para utilizar SageMaker Geospatial.

Uso de la política

Puede asociar AmazonSageMakerGeospatialExecutionRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 30 de noviembre de 2022 a las 10:08 UTC
- Hora de edición: 10 de mayo de 2023 a las 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*",
        "arn:aws:s3::*Sagemaker*",
        "arn:aws:s3::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetEarthObservationJob",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
    }
  ]
}
```



```
{
  "Effect" : "Allow",
  "Action" : "sagemaker-geospatial:GetRasterDataCollection",
  "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerGeospatialFullAccess

AmazonSageMakerGeospatialFullAccess es una [política administrada por AWS](#) que: concede permisos de acceso total a Amazon SageMaker Geospatial a través de la AWS Management Console y SDK.

Uso de la política

Puede asociar AmazonSageMakerGeospatialFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 30 de noviembre de 2022 a las 10:06 UTC
- Hora de edición: 30 de noviembre de 2022 a las 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker-geospatial.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerGroundTruthExecution

AmazonSageMakerGroundTruthExecution es una [política administrada por AWS](#) que: proporciona acceso a los servicios de AWS necesarios para realizar el trabajo de etiquetado de SageMaker GroundTruth

Uso de la política

Puede asociar AmazonSageMakerGroundTruthExecution a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de julio de 2020 a las 19:30 UTC
- Hora de edición: 29 de abril de 2022 a las 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Resource" : [
      "arn:aws:lambda:*:*:function:*GtRecipe*",
      "arn:aws:lambda:*:*:function:*LabelingFunction*",
      "arn:aws:lambda:*:*:function:*SageMaker*",
      "arn:aws:lambda:*:*:function:*sagemaker*",
      "arn:aws:lambda:*:*:function:*Sagemaker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*GroundTruth*",
      "arn:aws:s3::*Groundtruth*",
      "arn:aws:s3::*groundtruth*",
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/SageMaker" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket"
    ],
    "Resource" : "*"
  },
},

```

```
{
  "Sid" : "CloudWatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData",
    "logs:CreateLogStream",
    "logs:CreateLogGroup",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
},
{
  "Sid" : "StreamingQueue",
  "Effect" : "Allow",
  "Action" : [
    "sqs:CreateQueue",
    "sqs:DeleteMessage",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "sqs:ReceiveMessage",
    "sqs:SendMessage",
    "sqs:SetQueueAttributes"
  ],
  "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
},
{
  "Sid" : "StreamingTopicSubscribe",
  "Effect" : "Allow",
  "Action" : "sns:Subscribe",
  "Resource" : [
    "arn:aws:sns:*:*:*GroundTruth*",
    "arn:aws:sns:*:*:*Groundtruth*",
    "arn:aws:sns:*:*:*groundTruth*",
    "arn:aws:sns:*:*:*groundtruth*",
    "arn:aws:sns:*:*:*SageMaker*",
    "arn:aws:sns:*:*:*Sagemaker*",
    "arn:aws:sns:*:*:*sageMaker*",
    "arn:aws:sns:*:*:*sagemaker*"
  ],
  "Condition" : {
    "StringEquals" : {
      "sns:Protocol" : "sqs"
    }
  },
}
```

```

    "StringLike" : {
      "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
    }
  },
  {
    "Sid" : "StreamingTopic",
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : [
      "arn:aws:sns:*:*:*GroundTruth*",
      "arn:aws:sns:*:*:*Groundtruth*",
      "arn:aws:sns:*:*:*groundTruth*",
      "arn:aws:sns:*:*:*groundtruth*",
      "arn:aws:sns:*:*:*SageMaker*",
      "arn:aws:sns:*:*:*Sagemaker*",
      "arn:aws:sns:*:*:*sageMaker*",
      "arn:aws:sns:*:*:*sagemaker*"
    ]
  },
  {
    "Sid" : "StreamingTopicUnsubscribe",
    "Effect" : "Allow",
    "Action" : [
      "sns:Unsubscribe"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "WorkforceVPC",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint",
      "ec2:DescribeVpcEndpoints",
      "ec2>DeleteVpcEndpoints"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "ec2:VpceServiceName" : [
          "*sagemaker-task-resources*",
          "aws.sagemaker*labeling*"
        ]
      }
    }
  }
}

```

```
    ]
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerMechanicalTurkAccess

AmazonSageMakerMechanicalTurkAccess es una [política administrada por AWS](#) que: otorga acceso para crear recursos de Amazon Augmented AI FlowDefinition para cualquier equipo de trabajo.

Uso de la política

Puede asociar AmazonSageMakerMechanicalTurkAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 16:19 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerModelGovernanceUseAccess

AmazonSageMakerModelGovernanceUseAccess es una [política administrada por AWS](#) por la que: AWS concede los permisos necesarios para utilizar todas las características de Amazon SageMaker Governance. La política también brinda acceso selecto a los servicios relacionados (por ejemplo, S3 o KMS).

Uso de la política

Puede asociar `AmazonSageMakerModelGovernanceUseAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2022 a las 08:58 UTC
- Hora de edición: 17 de julio de 2023 a las 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker>DeleteModelCard",
        "sagemaker:ListModelCards",

```

```

    "sagemaker:ListModelCardVersions",
    "sagemaker:CreateModelCardExportJob",
    "sagemaker:DescribeModelCardExportJob",
    "sagemaker:ListModelCardExportJobs"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListTrainingJobs",
    "sagemaker:DescribeTrainingJob",
    "sagemaker:ListModels",
    "sagemaker:DescribeModel",
    "sagemaker:Search",
    "sagemaker:AddTags",
    "sagemaker>DeleteTags",
    "sagemaker:ListTags"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:CreateBucket",
    "s3:GetBucketLocation"
  ],
  "Resource" : [
    "arn:aws:s3:::*SageMaker*",
    "arn:aws:s3:::*Sagemaker*",
    "arn:aws:s3:::*sagemaker*"
  ]
},
{
  "Effect" : "Allow",

```

```
    "Action" : [
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerModelRegistryFullAccess

AmazonSageMakerModelRegistryFullAccess es una [política administrada por AWS](#) que es una nueva política administrada para Model Registry en SageMaker. Esta es una política independiente que se puede asociar al rol de usuario para acceder a las funcionalidades relacionadas con Model Registry en SageMaker.

Uso de la política

Puede asociar AmazonSageMakerModelRegistryFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de abril de 2023 a las 05:20 UTC
- Hora de edición: 13 de abril de 2023 a las 05:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerNotebooksServiceRolePolicy

AmazonSageMakerNotebooksServiceRolePolicy es una [política administrada por AWS](#) que es para el rol vinculado a un servicio para Amazon SageMaker Notebooks

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de octubre de 2019 a las 20:27 UTC
- Hora de edición: 09 de marzo de 2023 a las 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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" : "*"
}

```

```
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio utilizada por AWS APIGateway dentro de los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un conjunto de servicios relacionados, incluidos Lambda y otros.

Uso de la política

Puede asociar

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de agosto de 2023 a las 15:06 UTC
- Hora de edición: 1 de agosto de 2023 a las 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio utilizada por AWS CloudFormation dentro de los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un subconjunto de servicios relacionados, incluidos Lambda, APIGateway y otros.

Uso de la política

Puede asociar

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de agosto de 2023 a las 15:06 UTC
- Hora de edición: 1 de agosto de 2023 a las 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
```

```
    "lambda:UpdateFunctionCode",
    "lambda:ListTags",
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:sagemaker-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda:TagResource"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:sagemaker-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "sagemaker:project-name",
        "sagemaker:partner"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:PublishLayerVersion",
    "lambda:GetLayerVersion",
    "lambda>DeleteLayerVersion",
    "lambda:GetFunction"
  ],
}
```

```

    "Resource" : [
      "arn:aws:lambda:*:*:layer:sagemaker-*",
      "arn:aws:lambda:*:*:function:sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "apigateway:DELETE",
      "apigateway:PATCH",
      "apigateway:POST",
      "apigateway:PUT"
    ],
    "Resource" : [
      "arn:aws:apigateway:*:*/restapis/*",
      "arn:aws:apigateway:*:*/restapis"
    ],
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/sagemaker:project-name" : "false",
        "aws:ResourceTag/sagemaker:partner" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:POST",
      "apigateway:PUT"
    ],
    "Resource" : [
      "arn:aws:apigateway:*:*/restapis",
      "arn:aws:apigateway:*:*/tags/*"
    ],
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/sagemaker:project-name" : "false",
        "aws:ResourceTag/sagemaker:partner" : "false"
      },
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "sagemaker:project-name",
          "sagemaker:partner"
        ]
      }
    }
  }
}

```



```
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio que AWS Lambda usa en los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un conjunto de servicios relacionados, incluidos Secrets Manager y otros.

Uso de la política

Puede asociar

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de agosto de 2023 a las 15:05 UTC
- Hora de edición: 1 de agosto de 2023 a las 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerPipelinesIntegrations

AmazonSageMakerPipelinesIntegrations es una [política administrada por AWS](#). Esta política administrada por Amazon concede los permisos que normalmente se necesitan para su uso con los pasos de Callback y los pasos de Lambda en SageMaker Model Building Pipelines. Se añade al SageMaker-ExecutionRole de Amazon que se puede crear al configurar SageMaker Studio. También, se puede asociar a cualquier otro rol que se vaya a utilizar para crear o ejecutar pipelines.

Uso de la política

Puede asociar AmazonSageMakerPipelinesIntegrations a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de julio de 2021 a las 16:35 UTC
- Hora de edición: 17 de febrero de 2023 a las 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
        "arn:aws:lambda:*:*:function:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam:*:*:role/*",
      "Condition" : {
```

```

    "StringEquals" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "elasticmapreduce.amazonaws.com",
        "ec2.amazonaws.com"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:PutRule",
      "events:PutTargets"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
      "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:AddJobFlowSteps",
      "elasticmapreduce:CancelSteps",
      "elasticmapreduce:DescribeStep",
      "elasticmapreduce:RunJobFlow",
      "elasticmapreduce:DescribeCluster",
      "elasticmapreduce:TerminateJobFlows",
      "elasticmapreduce:ListSteps"
    ],
    "Resource" : [
      "arn:aws:elasticmapreduce:*:*:cluster/*"
    ]
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerReadOnly

AmazonSageMakerReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Amazon SageMaker a través de la AWS Management Console y SDK.

Uso de la política

Puede asociar AmazonSageMakerReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2017 a las 13:07 UTC
- Hora de edición: 1 de diciembre de 2021 a las 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

```

    "sagemaker:List*",
    "sagemaker:BatchGetMetrics",
    "sagemaker:GetDeviceRegistration",
    "sagemaker:GetDeviceFleetReport",
    "sagemaker:GetSearchSuggestions",
    "sagemaker:BatchGetRecord",
    "sagemaker:GetRecord",
    "sagemaker:Search",
    "sagemaker:QueryLineage",
    "sagemaker:GetLineageGroupPolicy",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:GetModelPackageGroupPolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "aws-marketplace:ViewSubscriptions",
    "cloudwatch:DescribeAlarms",
    "cognito-idp:DescribeUserPool",
    "cognito-idp:DescribeUserPoolClient",
    "cognito-idp:ListGroups",
    "cognito-idp:ListIdentityProviders",
    "cognito-idp:ListUserPoolClients",
    "cognito-idp:ListUserPools",
    "cognito-idp:ListUsers",
    "cognito-idp:ListUsersInGroup",
    "ecr:Describe*"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio utilizada por AWS APIGateway dentro de los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un conjunto de servicios relacionados, incluidos los Registros de CloudWatch y otros.

Uso de la política

Puede asociar

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de marzo de 2022 a las 04:25 UTC
- Hora de edición: 25 de marzo de 2022 a las 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs>DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio utilizada por AWS CloudFormation dentro de los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un subconjunto de servicios relacionados, incluidos SageMaker y otros.

Uso de la política

Puede asociar

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de marzo de 2022 a las 04:26 UTC
- Hora de edición: 25 de marzo de 2022 a las 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"sagemaker:AddTags",
"sagemaker:AssociateTrialComponent",
"sagemaker:BatchDescribeModelPackage",
"sagemaker:BatchGetMetrics",
"sagemaker:BatchGetRecord",
"sagemaker:BatchPutMetrics",
"sagemaker:CreateAction",
"sagemaker:CreateAlgorithm",
"sagemaker:CreateApp",
"sagemaker:CreateAppImageConfig",
"sagemaker:CreateArtifact",
"sagemaker:CreateAutoMLJob",
"sagemaker:CreateCodeRepository",
"sagemaker:CreateCompilationJob",
"sagemaker:CreateContext",
"sagemaker:CreateDataQualityJobDefinition",
"sagemaker:CreateDeviceFleet",
"sagemaker:CreateDomain",
"sagemaker:CreateEdgePackagingJob",
"sagemaker:CreateEndpoint",
"sagemaker:CreateEndpointConfig",
"sagemaker:CreateExperiment",
"sagemaker:CreateFeatureGroup",
"sagemaker:CreateFlowDefinition",
"sagemaker:CreateHumanTaskUi",
"sagemaker:CreateHyperParameterTuningJob",
"sagemaker:CreateImage",
"sagemaker:CreateImageVersion",
"sagemaker:CreateInferenceRecommendationsJob",
"sagemaker:CreateLabelingJob",
"sagemaker:CreateLineageGroupPolicy",
"sagemaker:CreateModel",
"sagemaker:CreateModelBiasJobDefinition",
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
```

```
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker>DeleteAction",
"sagemaker>DeleteAlgorithm",
"sagemaker>DeleteApp",
"sagemaker>DeleteAppImageConfig",
"sagemaker>DeleteArtifact",
"sagemaker>DeleteAssociation",
"sagemaker>DeleteCodeRepository",
"sagemaker>DeleteContext",
"sagemaker>DeleteDataQualityJobDefinition",
"sagemaker>DeleteDeviceFleet",
"sagemaker>DeleteDomain",
"sagemaker>DeleteEndpoint",
"sagemaker>DeleteEndpointConfig",
"sagemaker>DeleteExperiment",
"sagemaker>DeleteFeatureGroup",
"sagemaker>DeleteFlowDefinition",
"sagemaker>DeleteHumanLoop",
"sagemaker>DeleteHumanTaskUi",
"sagemaker>DeleteImage",
"sagemaker>DeleteImageVersion",
"sagemaker>DeleteLineageGroupPolicy",
"sagemaker>DeleteModel",
"sagemaker>DeleteModelBiasJobDefinition",
"sagemaker>DeleteModelExplainabilityJobDefinition",
"sagemaker>DeleteModelPackage",
"sagemaker>DeleteModelPackageGroup",
"sagemaker>DeleteModelPackageGroupPolicy",
"sagemaker>DeleteModelQualityJobDefinition",
"sagemaker>DeleteMonitoringSchedule",
"sagemaker>DeleteNotebookInstance",
"sagemaker>DeleteNotebookInstanceLifecycleConfig",
"sagemaker>DeletePipeline",
"sagemaker>DeleteProject",
"sagemaker>DeleteRecord",
"sagemaker>DeleteTags",
"sagemaker>DeleteTrial",
```

```
"sagemaker:DeleteTrialComponent",
"sagemaker:DeleteUserProfile",
"sagemaker:DeleteWorkforce",
"sagemaker:DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
```

```
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
```

```
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfile",
"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"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio que AWS CodeBuild usa dentro de los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un subconjunto de servicios relacionados, incluidos CodePipeline, CodeBuild y otros.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de marzo de 2022 a las 04:27 UTC
- Hora de edición: 25 de marzo de 2022 a las 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio que AWS CodePipeline usa dentro de los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un subconjunto de servicios relacionados, incluidos CodePipeline, CodeBuild y otros.

Uso de la política

Puede asociar

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de febrero de 2022 a las 09:53 UTC
- Hora de edición: 22 de febrero de 2022 a las 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio utilizada por AWS CloudWatch Events dentro de los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un subconjunto de servicios relacionados, incluidos CodePipeline y otros.

Uso de la política

Puede asociar AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de febrero de 2022 a las 09:53 UTC
- Hora de edición: 22 de febrero de 2022 a las 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio que Firehose de AWS usa en los productos aprovisionados por ServiceCatalog de AWS de la cartera de productos de Amazon SageMaker. Otorga permisos a un conjunto de servicios relacionados, incluidos Firehose y otros.

Uso de la política

Puede asociar AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de febrero de 2022 a las 09:54 UTC
- Hora de edición: 22 de febrero de 2022 a las 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
    "firehose:PutRecordBatch"
  ],
  "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio que AWS Glue usa en los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un conjunto de servicios relacionados, incluidos Glue, S3 y otros.

Uso de la política

Puede asociar AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de febrero de 2022 a las 09:51 UTC
- Hora de edición: 26 de agosto de 2022 a las 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue>DeletePartition",
        "glue>DeleteTable",
        "glue>DeleteTableVersion",
        "glue:GetDatabase",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:SearchTables",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/global_temp",

```

```

    "arn:aws:glue:*:*:database/sagemaker-*",
    "arn:aws:glue:*:*:table/sagemaker-*",
    "arn:aws:glue:*:*:tableVersion/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:DeleteBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3>ListAllMyBuckets",
    "s3>ListBucket",
    "s3>ListBucketMultipartUploads",
    "s3:PutBucketCors"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs>DeleteLogDelivery",

```

```
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy es una [política administrada por AWS](#) que: es una política de roles de servicio que AWS Lambda usa en los productos aprovisionados por AWS ServiceCatalog de la cartera de productos de Amazon SageMaker. Otorga permisos a un conjunto de servicios relacionados, incluidos ECR, S3 y otros.

Uso de la política

Puede asociar AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de abril de 2022 a las 16:34 UTC

- Hora de edición: 4 de abril de 2022 a las 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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/*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSecurityLakeAdministrator

AmazonSecurityLakeAdministrator es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Security Lake y a los servicios relacionados necesarios para administrar Security Lake.

Uso de la política

Puede asociar AmazonSecurityLakeAdministrator a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de mayo de 2023 a las 22:04 UTC
- Hora editada: 23 de febrero de 2024 a las 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
```

```
    "organizations:ListDelegatedServicesForAccount",
    "organizations:ListAccounts",
    "iam:ListRoles",
    "ram:GetResourceShareAssociations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateCrawler",
    "glue:StopCrawlerSchedule",
    "lambda:CreateEventSourceMapping",
    "lakeformation:GrantPermissions",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "lakeformation:GetDatalakeSettings",
    "events:ListConnections",
    "events:ListApiDestinations",
    "iam:GetRole",
    "iam:ListAttachedRolePolicies",
    "kms:DescribeKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowManagingSecurityLakeS3Buckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketNotification",
    "s3:PutBucketTagging",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketVersioning",
    "s3:PutReplicationConfiguration",
```



```

    "s3:PutLifecycleConfiguration",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:GetBucketNotification"
  ],
  "Resource" : "arn:aws:s3:::aws-security-data-lake*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowLambdaCreateFunction",
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
    "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowLambdaAddPermission",
  "Effect" : "Allow",
  "Action" : [
    "lambda:AddPermission"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
    "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    },
    "StringEquals" : {
      "lambda:Principal" : "securitylake.amazonaws.com"
    }
  }
}

```

```
    }
  }
},
{
  "Sid" : "AllowGlueActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue:GetDatabase",
    "glue:CreateTable",
    "glue:GetTable"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
    "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowEventBridgeActions",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:PutRule",
    "events:DescribeRule",
    "events:CreateApiDestination",
    "events:CreateConnection",
    "events:UpdateConnection",
    "events:UpdateApiDestination",
    "events>DeleteConnection",
    "events>DeleteApiDestination",
    "events:ListTargetsByRule",
    "events:RemoveTargets",
    "events>DeleteRule"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/AmazonSecurityLake*",
    "arn:aws:events:*:*:rule/SecurityLake*",
    "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
  ]
}
```

```

    "arn:aws:events:*:*:connection/AmazonSecurityLake*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowSQSActions",
  "Effect" : "Allow",
  "Action" : [
    "sqs:CreateQueue",
    "sqs:SetQueueAttributes",
    "sqs:GetQueueURL",
    "sqs:AddPermission",
    "sqs:GetQueueAttributes",
    "sqs>DeleteQueue"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:SecurityLake*",
    "arn:aws:sqs:*:*:AmazonSecurityLake*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowKmsCmkGrantForSecurityLake",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    },
    "StringLike" : {
      "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
    },
    "ForAllValues:StringEquals" : {
      "kms:GrantOperations" : [
        "GenerateDataKey",

```

```

        "RetireGrant",
        "Decrypt"
    ]
}
},
{
    "Sid" : "AllowEnablingQueryBasedSubscribers",
    "Effect" : "Allow",
    "Action" : [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLikeIfExists" : {
            "ram:ResourceArn" : [
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
                "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
            ]
        },
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "securitylake.amazonaws.com"
        }
    }
},
{
    "Sid" : "AllowConfiguringQueryBasedSubscribers",
    "Effect" : "Allow",
    "Action" : [
        "ram:UpdateResourceShare",
        "ram:GetResourceShares",
        "ram:DisassociateResourceShare",
        "ram>DeleteResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ram:ResourceShareName" : "LakeFormation*"
        },
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "securitylake.amazonaws.com"
        }
    }
}

```

```

    }
  },
  {
    "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition" : {

```

```

    "StringEquals" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    },
    "StringLike" : {
      "iam:AssociatedResourceARN" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ]
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "s3.amazonaws.com"
    },
    "StringLike" : {
      "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
    }
  }
},
{
  "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "s3.amazonaws.com"
    },
    "StringLike" : {
      "iam:AssociatedResourceARN" : "arn:aws:s3::*:aws-security-data-lake*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
}

```

```

    }
  }
},
{
  "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "glue.amazonaws.com"
    },
    "StringLike" : {
      "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
    }
  }
},
{
  "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "glue.amazonaws.com"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "events.amazonaws.com"
    },
    "StringLike" : {

```

```

        "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
    }
}
},
{
    "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
            "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "securitylake.amazonaws.com"
        }
    }
},
{
    "Sid" : "AllowOnboardingToSecurityLakeDependencies",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam:*:*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam:*:*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : [
                "securitylake.amazonaws.com",
                "lakeformation.amazonaws.com",
                "apidestinations.events.amazonaws.com"
            ]
        }
    }
},
},

```



```

{
  "Sid" : "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" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonSecurityLakeMetastoreManager

AmazonSecurityLakeMetastoreManager es una [política AWS gestionada](#) que: Política para el administrador de SecurityLake metatiendas de Amazon lambda que permite el acceso a cloudwatch, S3, Glue y SQS.

Uso de la política

Puede asociar AmazonSecurityLakeMetastoreManager a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 23 de enero de 2024 a las 15:26 UTC
- Hora editada: 23 de enero de 2024 a las 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
    "arn:aws:logs:*:*/aws/lambda/AmazonSecurityLake*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowGlueManage",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreatePartition",
    "glue:BatchCreatePartition",
    "glue:GetTable",
    "glue:UpdateTable"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
    "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
    "arn:aws:glue:*:*:catalog"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AllowToReadFromSqs",
  "Effect" : "Allow",
  "Action" : [
    "sqs:ReceiveMessage",
    "sqs>DeleteMessage",
    "sqs:GetQueueAttributes"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:AmazonSecurityLake*"
  ]
}

```

```

    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AllowMetaDataReadWrite",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-security-data-lake*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSecurityLakePermissionsBoundary

AmazonSecurityLakePermissionsBoundary es una [política administrada por AWS](#) por la que: Amazon Security Lake crea roles de IAM para que fuentes personalizadas de terceros escriban datos

en un lago de datos, y para que los suscriptores de terceros consuman datos de un lago de datos. A su vez, Amazon Security Lake utiliza esta política al crear estos roles para definir el límite de sus permisos.

Uso de la política

Puede asociar `AmazonSecurityLakePermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2022 a las 14:11 UTC
- Hora de edición: 29 de noviembre de 2022 a las 14:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSESFullAccess

AmazonSESFullAccess es una [política administrada por AWS](#) que: otorga acceso total a Amazon SES a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonSESPullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESPullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSESReadOnlyAccess

AmazonSESReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Amazon SES a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonSESReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "ses:Get*",
        "ses:List*"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSNSFullAccess

AmazonSNSFullAccess es una [política administrada por AWS](#) que: concede acceso total a Amazon SNS a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonSNSFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSNSReadOnlyAccess

AmazonSNSReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon SNS a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonSNSReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSNSRole

AmazonSNSRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio de Amazon SNS.

Uso de la política

Puede asociar AmazonSNSRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSQSFullAccess

AmazonSQSFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon SQS a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonSQSFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSQSReadOnlyAccess

AmazonSQSReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a Amazon SQS a través de la AWS Management Console.

Uso de la política

Puede asociar AmazonSQSReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 15 de junio de 2023 a las 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMAutomationApproverAccess

AmazonSSMAutomationApproverAccess es una [política administrada por AWS](#) que: proporciona acceso para ver ejecuciones de automatización y enviar decisiones de aprobación de automatización en espera de aprobación

Uso de la política

Puede asociar AmazonSSMAutomationApproverAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de agosto de 2017 a las 23:07 UTC
- Hora de edición: 7 de agosto de 2017 a las 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Action" : [
      "ssm:DescribeAutomationExecutions",
      "ssm:GetAutomationExecution",
      "ssm:SendAutomationSignal"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMAutomationRole

AmazonSSMAutomationRole es una [política administrada por AWS](#) que: otorga permisos para que el servicio de automatización de EC2 ejecute las actividades definidas en los documentos de automatización

Uso de la política

Puede asociar AmazonSSMAutomationRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de diciembre de 2016 a las 22:09 UTC
- Hora de edición: 24 de julio de 2017 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2>DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "cloudformation>DeleteStack"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:*"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : [
      "arn:aws:sns:*:*:Automation*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMDirectoryServiceAccess

AmazonSSMDirectoryServiceAccess es una [política administrada por AWS](#) que: permite que el agente SSM acceda a Directory Service en nombre del cliente para unirse al dominio de la instancia administrada.

Uso de la política

Puede asociar `AmazonSSMDirectoryServiceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de marzo de 2019 a las 17:44 UTC
- Hora de edición: 15 de marzo de 2019 a las 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMFullAccess

AmazonSSMFullAccess es una [política administrada por AWS](#) que: brinda acceso total a Amazon SSM.

Uso de la política

Puede asociar AmazonSSMFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de mayo de 2015 a las 17:39 UTC
- Hora de edición: 20 de noviembre de 2019 a las 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```

    "ds:CreateComputer",
    "ds:DescribeDirectories",
    "ec2:DescribeInstanceStatus",
    "logs:*",
    "ssm:*",
    "ec2messages:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "ssm.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssmmessages:CreateControlChannel",
    "ssmmessages:CreateDataChannel",
    "ssmmessages:OpenControlChannel",
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMMaintenanceWindowRole

AmazonSSMMaintenanceWindowRole es una [política administrada por AWS](#) que: es un rol de servicio que se utilizará en la ventana de mantenimiento de EC2

Uso de la política

Puede asociar AmazonSSMMaintenanceWindowRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2016 a las 15:57 UTC
- Hora de edición: 27 de julio de 2019 a las 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution",
      "ssm:GetParameters",
      "ssm:ListCommands",
      "ssm:SendCommand",
      "ssm:StartAutomationExecution"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:SSM*",
      "arn:aws:lambda:*:*:function:*:SSM*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "states:DescribeExecution",
      "states:StartExecution"
    ],
    "Resource" : [
      "arn:aws:states:*:*:stateMachine:SSM*",
      "arn:aws:states:*:*:execution:SSM*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:ListGroup",
      "resource-groups:ListGroupResources"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMManagedEC2InstanceDefaultPolicy

AmazonSSMManagedEC2InstanceDefaultPolicy es una [política administrada por AWS](#) que: habilita la funcionalidad de AWS Systems Manager en las instancias EC2.

Uso de la política

Puede asociar AmazonSSMManagedEC2InstanceDefaultPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de agosto de 2022 a las 20:54 UTC
- Hora de edición: 30 de agosto de 2022 a las 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMManagedInstanceCore

AmazonSSMManagedInstanceCore es una [política administrada por AWS](#) que: es un rol de Amazon EC2 para habilitar las funciones principales del servicio AWS Systems Manager.

Uso de la política

Puede asociar AmazonSSMManagedInstanceCore a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de marzo de 2019 a las 17:22 UTC
- Hora de edición: 23 de mayo de 2019 a las 16:54 UTC

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

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
```

```
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2messages:AcknowledgeMessage",
    "ec2messages:DeleteMessage",
    "ec2messages:FailMessage",
    "ec2messages:GetEndpoint",
    "ec2messages:GetMessages",
    "ec2messages:SendReply"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMPatchAssociation

AmazonSSMPatchAssociation es una [política administrada por AWS](#) que: proporciona acceso a las instancias secundarias para realizar la asociación de parches.

Uso de la política

Puede asociar AmazonSSMPatchAssociation a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 13 de mayo de 2020 a las 16:00 UTC
- Hora de edición: 13 de mayo de 2020 a las 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribeEffectivePatchesForPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMReadOnlyAccess

AmazonSSMReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a SSM de Amazon.

Uso de la política

Puede asociar AmazonSSMReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de mayo de 2015 a las 17:44 UTC
- Hora de edición: 29 de mayo de 2015 a las 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:Describe*",
      "ssm:Get*",
      "ssm:List*"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSSMServiceRolePolicy

AmazonSSMServiceRolePolicy es una [política administrada por AWS](#) que: brinda acceso a los recursos de AWS administrados o utilizados por Amazon SSM

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de noviembre de 2017 a las 19:20 UTC
- Hora de edición: 14 de septiembre de 2022 a las 19:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceState",
    "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" : "*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonSumerianFullAccess

AmazonSumerianFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Sumerian.

Uso de la política

Puede asociar AmazonSumerianFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de abril de 2018 a las 20:14 UTC
- Hora de edición: 24 de abril de 2018 a las 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonTextractFullAccess

AmazonTextractFullAccess es una [política administrada por AWS](#) que: brinda acceso a todas las API de Amazon Textract

Uso de la política

Puede asociar AmazonTextractFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2018 a las 19:07 UTC
- Hora de edición: 28 de noviembre de 2018 a las 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTexttractFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonTextractServiceRole

AmazonTextractServiceRole es una [política administrada por AWS](#) que: permite que Textract llame a los servicios de AWS en su nombre.

Uso de la política

Puede asociar AmazonTextractServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de noviembre de 2018 a las 19:12 UTC
- Hora de edición: 28 de noviembre de 2018 a las 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonTimestreamConsoleFullAccess

AmazonTimestreamConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total para gestionar Amazon Timestream mediante la AWS Management Console. Tenga en cuenta que esta política también otorga permisos para determinadas operaciones de KMS y para las operaciones que administran las consultas guardadas. Si utiliza una CMK gestionada por el cliente, consulte la documentación para obtener los permisos adicionales necesarios.

Uso de la política

Puede asociar AmazonTimestreamConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de septiembre de 2020 a las 21:47 UTC
- Hora de edición: 1 de febrero de 2022 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "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" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonTimestreamFullAccess

AmazonTimestreamFullAccess es una [política administrada por AWS](#) que: brinda acceso total a Amazon Timestream. Tenga en cuenta que esta política también otorga acceso a determinadas operaciones de KMS. Si utiliza una CMK gestionada por el cliente, consulte la documentación para obtener los permisos adicionales necesarios.

Uso de la política

Puede asociar AmazonTimestreamFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de septiembre de 2020 a las 21:47 UTC
- Hora de edición: 26 de noviembre de 2021 a las 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    }
  ],
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonTimestreamInfluxDBFullAccess

AmazonTimestreamInfluxDBFullAccesses una [política AWS gestionada](#) que: proporciona acceso administrativo completo para crear, actualizar, eliminar y enumerar instancias de Amazon Timestream InfluxDB y crear y enumerar grupos de parámetros. Consulte la documentación para obtener los permisos adicionales necesarios.

Uso de la política

Puede asociar AmazonTimestreamInfluxDBFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de marzo de 2024 a las 22:53 UTC
- Hora editada: 14 de marzo de 2024 a las 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```

    "timestream-influxdb:CreateDbParameterGroup",
    "timestream-influxdb:GetDbParameterGroup",
    "timestream-influxdb:ListDbParameterGroups",
    "timestream-influxdb:CreateDbInstance",
    "timestream-influxdb>DeleteDbInstance",
    "timestream-influxdb:GetDbInstance",
    "timestream-influxdb:ListDbInstances",
    "timestream-influxdb:TagResource",
    "timestream-influxdb:UntagResource",
    "timestream-influxdb:ListTagsForResource",
    "timestream-influxdb:UpdateDbInstance"
  ],
  "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:::*"
  ]
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonTimestreamInfluxDBServiceRolePolicy

AmazonTimestreamInfluxDBServiceRolePolicy es una [política AWS gestionada](#) que proporciona acceso administrativo completo para crear, actualizar, eliminar y enumerar instancias de

Amazon Timestream InfluxDB y crear y enumerar grupos de parámetros. Consulte la documentación para obtener los permisos adicionales necesarios.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de marzo de 2024 a las 18:53 UTC
- Hora editada: 14 de marzo de 2024 a las 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
```

```

    "Sid" : "CreateEniInSubnetStatement",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Sid" : "CreateEniStatement",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
      }
    }
  },
  {
    "Sid" : "CreateTagWithEniStatement",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
      },
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateNetworkInterface"
        ]
      }
    }
  },
  {
    "Sid" : "ManageEniStatement",
    "Effect" : "Allow",

```

```

    "Action" : [
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
      }
    }
  },
  {
    "Sid" : "PutCloudWatchMetricsStatement",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Timestream/InfluxDB",
          "AWS/Usage"
        ]
      }
    }
  },
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ManageSecretStatement",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager>DeleteSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}

```

```
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonTimestreamReadOnlyAccess

AmazonTimestreamReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Timestream. La política también proporciona permiso para cancelar cualquier consulta en curso. Si utiliza una CMK gestionada por el cliente, consulte la documentación para obtener los permisos adicionales necesarios.

Uso de la política

Puede asociar AmazonTimestreamReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de septiembre de 2020 a las 21:47 UTC
- Hora de edición: 28 de febrero de 2023 a las 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonTranscribeFullAccess

AmazonTranscribeFullAccess es una [política administrada por AWS](#) que: otorga acceso total a las operaciones de Amazon Transcribe

Uso de la política

Puede asociar AmazonTranscribeFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de abril de 2018 a las 16:06 UTC
- Hora de edición: 4 de abril de 2018 a las 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*transcribe*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonTranscribeReadOnlyAccess

AmazonTranscribeReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura a la operación de Amazon Transcribe

Uso de la política

Puede asociar AmazonTranscribeReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de abril de 2018 a las 16:05 UTC
- Hora de edición: 4 de abril de 2018 a las 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

AmazonVPCCrossAccountNetworkInterfaceOperations es una [política administrada por AWS](#) que: proporciona acceso para crear interfaces de red y asociarlas a recursos multicuenta

Uso de la política

Puede asociar AmazonVPCCrossAccountNetworkInterfaceOperations a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de julio de 2017 a las 20:47 UTC
- Hora de edición: 25 de septiembre de 2023 a las 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:CreateRoute",
        "ec2>DeleteRoute",
        "ec2:ReplaceRoute"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```

```
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeNetworkInterfacePermissions",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeRegions",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses",
    "ec2:UnassignPrivateIpAddresses"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses",
    "ec2:UnassignIpv6Addresses"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonVPCFullAccess

AmazonVPCFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a Amazon VPC a través de. AWS Management Console

Uso de la política

Puede asociar AmazonVPCFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora editada: 8 de febrero de 2024 a las 16:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
```

```
"ec2:AssignIpv6Addresses",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2: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" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy es una [política administrada por AWS](#) que: brinda permisos para describir los recursos de AWS, ejecutar el Analizador de acceso a la red y crear o eliminar etiquetas en Network Insights Access Scope y Network Insights Access Scope Analysis.

Uso de la política

Puede asociar `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de junio de 2023 a las 22:56 UTC
- Hora de edición: 3 de noviembre de 2023 a las 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

AmazonVPCReachabilityAnalyzerFullAccessPolicy es una [política administrada AWS](#) que: proporciona permisos para describir los recursos de AWS, ejecutar Reachability Analyzer y crear o eliminar etiquetas en Network Insights Path y Network Insights Analysis.

Uso de la política

Puede asociar AmazonVPCReachabilityAnalyzerFullAccessPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de junio de 2023 a las 20:12 UTC
- Hora de edición: 3 de noviembre de 2023 a las 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy es una [política administrada por AWS](#) que: está asociada al rol IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Este rol se implementa en las cuentas de los miembros de una organización, cuando la cuenta de administración permite el acceso confiable a Reachability Analyzer. Proporciona permisos para ver los recursos de toda la organización con la consola Reachability Analyzer.

Uso de la política

Puede asociar `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de mayo de 2023 a las 20:38 UTC
- Hora de edición: 1 de mayo de 2023 a las 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonVPCReadOnlyAccess

AmazonVPCReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a Amazon VPC a través de. AWS Management Console

Uso de la política

Puede asociar AmazonVPCReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora editada: 8 de febrero de 2024 a las 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Sid" : "AmazonVPCReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAddresses",
      "ec2:DescribeCarrierGateways",
      "ec2:DescribeClassicLinkInstances",
      "ec2:DescribeCustomerGateways",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeEgressOnlyInternetGateways",
      "ec2:DescribeFlowLogs",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeLocalGatewayRouteTables",
      "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
      "ec2:DescribeMovingAddresses",
      "ec2:DescribeNatGateways",
      "ec2:DescribeNetworkAcls",
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeNetworkInterfacePermissions",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribePrefixLists",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroupReferences",
      "ec2:DescribeSecurityGroupRules",
      "ec2:DescribeSecurityGroups",
      "ec2: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" : "*"    
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AmazonWorkDocsFullAccess

AmazonWorkDocsFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon WorkDocs a través de la AWS Management Console

Uso de la política

Puede asociar AmazonWorkDocsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 16 de abril de 2020 a las 23:05 UTC
- Hora de edición: 16 de abril de 2020 a las 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkDocsReadOnlyAccess

AmazonWorkDocsReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon WorkDocs a través de la AWS Management Console

Uso de la política

Puede asociar AmazonWorkDocsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de enero de 2020 a las 23:49 UTC
- Hora de edición: 8 de enero de 2020 a las 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkMailEventsServiceRolePolicy

AmazonWorkMailEventsServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los recursos de Servicios de AWS utilizados o gestionados por Amazon WorkMail Events

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de abril de 2019 a las 16:52 UTC
- Hora de edición: 16 de abril de 2019 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkMailFullAccess

AmazonWorkMailFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a WorkMail, Directory Service, SES y EC2 y acceso de lectura a los metadatos de KMS.

Uso de la política

Puede asociar AmazonWorkMailFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 21 de diciembre de 2020 a las 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds>DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteSubnet",
        "ec2>DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
```

```

    "route53:ListResourceRecordSets",
    "route53:GetHostedZone",
    "route53domains:CheckDomainAvailability",
    "route53domains:ListDomains",
    "ses:*",
    "workmail:*",
    "iam:ListRoles",
    "logs:DescribeLogGroups",
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy",
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "events.workmail.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*workmail*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "events.workmail.amazonaws.com"
    }
  }
}
]

```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkMailMessageFlowFullAccess

AmazonWorkMailMessageFlowFullAccess es una [política administrada por AWS](#) que: brinda acceso total a las API de WorkMail Message Flow

Uso de la política

Puede asociar AmazonWorkMailMessageFlowFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de febrero de 2021 a las 11:08 UTC
- Hora de edición: 11 de febrero de 2021 a las 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkMailMessageFlowReadOnlyAccess

AmazonWorkMailMessageFlowReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a los mensajes de WorkMail para la API GetRawMessageContent

Uso de la política

Puede asociar AmazonWorkMailMessageFlowReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de enero de 2021 a las 12:40 UTC
- Hora de edición: 28 de enero de 2021 a las 12:40 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkMailReadOnlyAccess

`AmazonWorkMailReadOnlyAccess` es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a WorkMail y SES.

Uso de la política

Puede asociar `AmazonWorkMailReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 25 de julio de 2019 a las 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkSpacesAdmin

AmazonWorkSpacesAdmin es una [política administrada por AWS](#) que: proporciona acceso a las acciones administrativas de Amazon WorkSpaces mediante SDK y CLI de AWS.

Uso de la política

Puede asociar AmazonWorkSpacesAdmin a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de septiembre de 2015 a las 22:21 UTC
- Hora de edición: 3 de agosto de 2023 a las 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkSpacesApplicationManagerAdminAccess

AmazonWorkSpacesApplicationManagerAdminAccess es una [política administrada por AWS](#) que: concede acceso de administrador para empaquetar una aplicación en Amazon WorkSpaces Application Manager.

Uso de la política

Puede asociar AmazonWorkSpacesApplicationManagerAdminAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de abril de 2015 a las 14:03 UTC
- Hora de edición: 09 de abril de 2015 a las 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Effect" : "Allow",
    "Action" : "wam:AuthenticatePackager",
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkspacesPCAAccess

AmazonWorkspacesPCAAccess es una [política administrada por AWS](#) que: proporciona acceso administrativo total a los recursos de AWS Certificate Manager Private CA que tiene su Cuenta de AWS para la autenticación basada en certificados.

Uso de la política

Puede asociar AmazonWorkspacesPCAAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de noviembre de 2022 a las 00:25 UTC
- Hora de edición: 8 de noviembre de 2022 a las 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkSpacesSelfServiceAccess

AmazonWorkSpacesSelfServiceAccess es una [política administrada por AWS](#) que: proporciona acceso al servicio de backend de Amazon WorkSpaces para realizar acciones de Workspace Self Service

Uso de la política

Puede asociar AmazonWorkSpacesSelfServiceAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2019 a las 19:22 UTC
- Hora de edición: 27 de junio de 2019 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkSpacesServiceAccess

AmazonWorkSpacesServiceAccess es una [política administrada por AWS](#) que: proporciona acceso a las cuentas de los clientes al servicio WorkSpaces de AWS para lanzar un espacio de trabajo.

Uso de la política

Puede asociar AmazonWorkSpacesServiceAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2019 a las 19:19 UTC
- Hora de edición: 18 de marzo de 2020 a las 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkSpacesWebReadOnly

AmazonWorkSpacesWebReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Amazon WorkSpaces Web y sus dependencias a través de SDK y CLI de AWS Management Console.

Uso de la política

Puede asociar AmazonWorkSpacesWebReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 30 de noviembre de 2021 a las 14:20 UTC
- Hora de edición: 2 de noviembre de 2022 a las 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "kinesis:ListStreams"
  ],
  "Resource" : "*"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonWorkSpacesWebServiceRolePolicy

AmazonWorkSpacesWebServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los Servicios de AWS y los recursos utilizados o gestionados por Amazon WorkSpaces Web

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2021 a las 13:15 UTC
- Hora de edición: 15 de diciembre de 2022 a las 22:46 UTC

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

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ],
  {
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:CreateNetworkInterface"
],
"Resource" : "arn:aws:ec2:*:*:network-interface/*",
"Condition" : {
  "StringEquals" : {
    "aws:RequestTag/WorkSpacesWebManaged" : "true"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "WorkSpacesWebManaged"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/WorkSpacesWebManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/WorkSpacesWeb",
          "AWS/Usage"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:PutRecord",
      "kinesis:PutRecords",
      "kinesis:DescribeStreamSummary"
    ],
    "Resource" : "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonZocaloFullAccess

AmazonZocaloFullAccess es una [política administrada por AWS](#) que: otorga acceso total a Amazon Zocalo.

Uso de la política

Puede asociar AmazonZocaloFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:*",
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmazonZocaloReadOnlyAccess

AmazonZocaloReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Zocalo

Uso de la política

Puede asociar AmazonZocaloReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AmplifyBackendDeployFullAccess

AmplifyBackendDeployFullAccesses una [política AWS gestionada](#) que: proporciona permisos de acceso total a Amplify para implementar los recursos de backend de Amplify (Amazon AWS AppSync Cognito, Amazon S3 y otros servicios relacionados) a través del kit de desarrollo (CDK) Nube de AWS AWS

Uso de la política

Puede asociar AmplifyBackendDeployFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de octubre de 2023 a las 21:32 UTC
- Hora de edición: 2 de enero de 2024 a las 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

APIGatewayServiceRolePolicy

APIGatewayServiceRolePolicy es una [política administrada por AWS](#) que: permite que la Puerta de enlace de la API gestione los recursos de AWS asociados en nombre del cliente.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de octubre de 2017 a las 17:23 UTC
- Hora de edición: 12 de julio de 2021 a las 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : [
```

```
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
    ],
    "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "acm:DescribeCertificate",
        "acm:GetCertificate"
    ],
    "Resource" : "arn:aws:acm:*:*:certificate/*"
},
{
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterfacePermission",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "Owner",
                "VpcLinkId"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
```

```
    "ec2:CreateNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeVpcs",
    "ec2:DescribeNetworkInterfacePermissions",
    "ec2:UnassignPrivateIpAddresses",
    "ec2:DescribeSubnets",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "servicediscovery:GetNamespace",
  "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
},
{
  "Effect" : "Allow",
  "Action" : "servicediscovery:GetService",
  "Resource" : "arn:aws:servicediscovery:*:*:service/*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AppIntegrationsServiceLinkedRolePolicy

AppIntegrationsServiceLinkedRolePolicy es una [política administrada por AWS](#) que permite que AppIntegrations gestione los recursos de AppFlow y publique datos de métricas de CloudWatch en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de septiembre de 2022 a las 19:42 UTC
- Hora de edición: 30 de septiembre de 2022 a las 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Action" : [
      "appflow:DescribeConnectorEntity",
      "appflow:ListConnectorEntities"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "appflow:DescribeConnectorProfiles",
      "appflow:UseConnectorProfile"
    ],
    "Resource" : "arn:aws:appflow:*:*:connector-profile/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "appflow>DeleteFlow",
      "appflow:DescribeFlow",
      "appflow:DescribeFlowExecutionRecords",
      "appflow:StartFlow",
      "appflow:StopFlow",
      "appflow:UpdateFlow"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AppIntegrationsManaged" : "true"
      }
    },
    "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "appflow:TagResource"
    ],
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "AppIntegrationsManaged"
        ]
      }
    },
    "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
  }

```

```
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ApplicationAutoScalingForAmazonAppStreamAccess

ApplicationAutoScalingForAmazonAppStreamAccess es una [política administrada por AWS](#) que: habilita el escalado automático de aplicaciones para Amazon AppStream

Uso de la política

Puede asociar ApplicationAutoScalingForAmazonAppStreamAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2017 a las 21:39 UTC
- Hora de edición: 6 de febrero de 2017 a las 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y los Recursos utilizados o administrados por la característica de exportación continua de Application Discovery Service

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de agosto de 2018 a las 20:22 UTC
- Hora de edición: 13 de agosto de 2018 a las 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
```

```

    "firehose:DescribeDeliveryStream",
    "logs:CreateLogGroup"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "firehose>DeleteDeliveryStream",
    "firehose:PutRecord",
    "firehose:PutRecordBatch",
    "firehose:UpdateDestination"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
},
{
  "Action" : [
    "s3:CreateBucket",
    "s3:ListBucket",
    "s3:PutBucketLogging",
    "s3:PutEncryptionConfiguration"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
},
{
  "Action" : [
    "s3:GetObject"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
},
{
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutRetentionPolicy"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
},
{

```

```
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "firehose.amazonaws.com"
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "firehose.amazonaws.com"
      }
    }
  }
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AppRunnerNetworkingServiceRolePolicy

AppRunnerNetworkingServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS AppRunner Networking administre los recursos de AWS relacionados en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de enero de 2022 a las 21:02 UTC
- Hora de edición: 12 de enero de 2022 a las 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
  ],
}
```



```
"Effect" : "Allow",
"Action" : "ec2:CreateNetworkInterface",
"Resource" : "*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "AWSAppRunnerManaged"
    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "StringLike" : {
      "aws:RequestTag/AWSAppRunnerManaged" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2>DeleteNetworkInterface",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AppRunnerServiceRolePolicy

AppRunnerServiceRolePolicy es una [política administrada por AWS](#) que: permite que AppRunner de AWS administre los recursos de AWS relacionados en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de mayo de 2021 a las 19:15 UTC
- Hora de edición: 14 de mayo de 2021 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events>DeleteRule",
    "events:RemoveTargets",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AutoScalingConsoleFullAccess

AutoScalingConsoleFullAccess es una [política administrada por AWS](#) que: brinda acceso total al escalado automático a través de la AWS Management Console.

Uso de la política

Puede asociar AutoScalingConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de enero de 2017 a las 19:43 UTC
- Hora de edición: 6 de febrero de 2018 a las 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:ImportKeyPair"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:Describe*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:ListMetrics",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:Describe*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "autoscaling:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:ListSubscriptions",
      "sns:ListTopics"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:ListRoles",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "autoscaling.amazonaws.com"
      }
    }
  }
}
```

```
    }  
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AutoScalingConsoleReadOnlyAccess

AutoScalingConsoleReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura al escalado automático a través de la AWS Management Console.

Uso de la política

Puede asociar AutoScalingConsoleReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de enero de 2017 a las 19:48 UTC
- Hora de edición: 12 de enero de 2017 a las 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AutoScalingFullAccess

AutoScalingFullAccess es una [política administrada por AWS](#) que: brinda acceso total al escalado automático.

Uso de la política

Puede asociar AutoScalingFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de enero de 2017 a las 19:31 UTC
- Hora de edición: 6 de febrero de 2018 a las 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "autoscaling.amazonaws.com"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AutoScalingNotificationAccessRole

AutoScalingNotificationAccessRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio de acceso a notificaciones de AutoScaling.

Uso de la política

Puede asociar AutoScalingNotificationAccessRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AutoScalingReadOnlyAccess

AutoScalingReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura al escalado automático.

Uso de la política

Puede asociar `AutoScalingReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de enero de 2017 a las 19:39 UTC
- Hora de edición: 12 de enero de 2017 a las 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AutoScalingServiceRolePolicy

AutoScalingServiceRolePolicy es una [política AWS administrada](#) que: permite el acceso Servicios de AWS y los recursos utilizados o administrados por Auto Scaling

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de enero de 2018 a las 23:10 UTC
- Hora de edición: 29 de febrero de 2024 a las 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
```

```

    "ec2:AttachClassicLinkVpc",
    "ec2:CancelSpotInstanceRequests",
    "ec2:CreateFleet",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:Describe*",
    "ec2:DetachClassicLinkVpc",
    "ec2:GetInstanceTypesFromInstanceRequirements",
    "ec2:GetSecurityGroupsForVpc",
    "ec2:ModifyInstanceAttribute",
    "ec2:RequestSpotInstances",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2InstanceProfileManagement",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ec2.amazonaws.com*"
    }
  }
},
{
  "Sid" : "EC2SpotManagement",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "spot.amazonaws.com"
    }
  }
},

```

```
{
  "Sid" : "ELBManagement",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:Register*",
    "elasticloadbalancing:Deregister*",
    "elasticloadbalancing:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CWManagement",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SNSManagement",
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EventBridgeRuleManagement",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "events>DeleteRule",
    "events:DescribeRule"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "autoscaling.amazonaws.com"
    }
  }
}
```

```

    }
  },
  {
    "Sid" : "SystemsManagerParameterManagement",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameters"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "VpcLatticeManagement",
    "Effect" : "Allow",
    "Action" : [
      "vpc-lattice:DeregisterTargets",
      "vpc-lattice:GetTargetGroup",
      "vpc-lattice:ListTargets",
      "vpc-lattice:ListTargetGroups",
      "vpc-lattice:RegisterTargets"
    ],
    "Resource" : "*"
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWS_ConfigRole

AWS_ConfigRole es una [política AWS administrada que: Política](#) predeterminada para el rol de servicio AWS Config. Proporciona los permisos necesarios para que AWS Config realice un seguimiento de los cambios en sus AWS recursos.

Uso de la política

Puede asociar AWS_ConfigRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 15 de septiembre de 2020 a las 20:30 UTC
- Hora de edición: 22 de febrero de 2024 a las 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Versión de la política

Versión de la política: v30 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
```

```
"airflow:ListTagsForResource",
"amplify:GetApp",
"amplify:GetBranch",
"amplify:ListApps",
"amplify:ListBranches",
"amplifyuibuilder:ExportThemes",
"amplifyuibuilder:GetTheme",
"amplifyuibuilder:ListThemes",
"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/*"
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSAccountActivityAccess

AWSAccountActivityAccess es una [política administrada por AWS](#) que: permite a los usuarios acceder a la página de actividad de la cuenta.

Uso de la política

Puede asociar AWSAccountActivityAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 7 de marzo de 2023 a las 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAccountManagementFullAccess

AWSAccountManagementFullAccess es una [política administrada por AWS](#) que: otorga acceso completo a la gestión de cuentas de AWS.

Uso de la política

Puede asociar AWSAccountManagementFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de septiembre de 2021 a las 23:20 UTC
- Hora de edición: 30 de septiembre de 2021 a las 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAccountManagementReadOnlyAccess

AWSAccountManagementReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a la administración de cuentas de AWS

Uso de la política

Puede asociar AWSAccountManagementReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de septiembre de 2021 a las 23:29 UTC
- Hora de edición: 30 de septiembre de 2021 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAccountUsageReportAccess

AWSAccountUsageReportAccess es una [política administrada por AWS](#) que: permite a los usuarios acceder a la página del informe de uso de la cuenta.

Uso de la política

Puede asociar AWSAccountUsageReportAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC

- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAgentlessDiscoveryService

AWSAgentlessDiscoveryService es una [política administrada por AWS](#) que: proporciona acceso al Discovery Agentless Connector para registrarse en AWS Application Discovery Service.

Uso de la política

Puede asociar AWSAgentlessDiscoveryService a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de agosto de 2016 a las 01:35 UTC
- Hora de edición: 24 de febrero de 2020 a las 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
```

```

    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::connector-platform-upgrade-info/*",
      "arn:aws:s3:::connector-platform-upgrade-info",
      "arn:aws:s3:::connector-platform-upgrade-bundles/*",
      "arn:aws:s3:::connector-platform-upgrade-bundles",
      "arn:aws:s3:::connector-platform-release-notes/*",
      "arn:aws:s3:::connector-platform-release-notes",
      "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
      "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource" : [
      "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "SNS:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
  },
  {
    "Sid" : "Discovery",
    "Effect" : "Allow",
    "Action" : [
      "Discovery:*"
    ],
    "Resource" : "*"
  },
},

```

```
{
  "Sid" : "arsenal",
  "Effect" : "Allow",
  "Action" : [
    "arsenal:RegisterOnPremisesAgent"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "mgh:GetHomeRegion"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppFabricFullAccess

AWSAppFabricFullAccess es una [política administrada por AWS](#) que: brinda acceso total al servicio AWS AppFabric y acceso de solo lectura a los servicios dependientes, como S3, Kinesis y KMS.

Uso de la política

Puede asociar AWSAppFabricFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2023 a las 19:51 UTC
- Hora de edición: 27 de junio de 2023 a las 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
```

```
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "FirehoseReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "firehose:DescribeDeliveryStream",
    "firehose:ListDeliveryStreams"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowUseOfServiceLinkedRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "appfabric.amazonaws.com"
    }
  },
  "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppFabricReadOnlyAccess

AWSAppFabricReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AppFabric de AWS

Uso de la política

Puede asociar AWSAppFabricReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2023 a las 19:52 UTC
- Hora de edición: 27 de junio de 2023 a las 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",

```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppFabricServiceRolePolicy

AWSAppFabricServiceRolePolicy es una [política administrada por AWS](#) que: proporciona a AppFabric acceso a los recursos de AWS en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de junio de 2023 a las 21:07 UTC
- Hora de edición: 26 de junio de 2023 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEmitMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppFabric"
        }
      }
    },
    {
      "Sid" : "S3PutObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3::*/AWSAppFabric/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FirehosePutRecord",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
      "Condition" : {
```

```
    "StringEqualsIgnoreCase" : {  
      "aws:ResourceTag/AWSAppFabricManaged" : "true"  
    }  
  }  
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

AWSApplicationAutoscalingAppStreamFleetPolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a AppStream y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de octubre de 2017 a las 19:04 UTC
- Hora de edición: 20 de octubre de 2017 a las 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingCassandraTablePolicy

AWSApplicationAutoscalingCassandraTablePolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a Cassandra y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de marzo de 2020 a las 22:49 UTC
- Hora de edición: 18 de marzo de 2020 a las 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cassandra:Select",
      "Resource" : [
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Alter",
```



```
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

AWSApplicationAutoscalingComprehendEndpointPolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a Comprehend y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2019 a las 18:39 UTC
- Hora de edición: 14 de noviembre de 2019 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoScalingCustomResourcePolicy

AWSApplicationAutoScalingCustomResourcePolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a APIGateway y CloudWatch para tener un escalado de recursos personalizado

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de junio de 2018 a las 23:22 UTC
- Hora de edición: 4 de junio de 2018 a las 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

AWSApplicationAutoscalingDynamoDBTablePolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a DynamoDB y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de octubre de 2017 a las 21:34 UTC
- Hora de edición: 20 de octubre de 2017 a las 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy es una [política administrada AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a la Flota de spot EC2 y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 25 de octubre de 2017 a las 18:23 UTC
- Hora de edición: 25 de octubre de 2017 a las 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingECSServicePolicy

AWSApplicationAutoscalingECSServicePolicy es una [política administrada por AWS](#) que otorga permisos al escalado automático de la aplicación para acceder a EC2 Container Service y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de octubre de 2017 a las 23:53 UTC
- Hora de edición: 25 de octubre de 2017 a las 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
```

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingElastiCacheRGPolicy

AWSApplicationAutoscalingElastiCacheRGPolicy es una [política administrada por AWS](#) que: concede permisos al escalado automático de la aplicación para acceder a Amazon ElastiCache y Amazon CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de agosto de 2021 a las 23:41 UTC
- Hora de edición: 17 de agosto de 2021 a las 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingEMRInstanceGroupPolicy

AWSApplicationAutoscalingEMRInstanceGroupPolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a Elastic Map Reduce y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de octubre de 2017 a las 00:57 UTC
- Hora de edición: 26 de octubre de 2017 a las 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
```

```
    "cloudwatch:DeleteAlarms"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingKafkaClusterPolicy

AWSApplicationAutoscalingKafkaClusterPolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a Managed Streaming para Apache Kafka y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de agosto de 2020 a las 18:36 UTC
- Hora de edición: 24 de agosto de 2020 a las 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

AWSApplicationAutoscalingLambdaConcurrencyPolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a Lambda y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de octubre de 2019 a las 20:04 UTC
- Hora de edición: 21 de octubre de 2019 a las 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda>DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

AWSApplicationAutoscalingNeptuneClusterPolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de la aplicación para acceder a Amazon Neptune y Amazon CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de septiembre de 2021 a las 21:14 UTC
- Hora de edición: 2 de septiembre de 2021 a las 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterParameters",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:AddTagsToResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:CreateDBInstance",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*",
        "arn:aws:rds:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DeleteDBInstance"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:db:autoscaled-reader*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
  ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingRDSClusterPolicy

AWSApplicationAutoscalingRDSClusterPolicy es una [política administrada por AWS](#) que otorga permisos al escalado automático de la aplicación para acceder a RDS y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de octubre de 2017 a las 17:46 UTC
- Hora de edición: 7 de agosto de 2018 a las 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CreateDBInstance",
        "rds>DeleteDBInstance",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:ModifyDBCluster",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "rds.amazonaws.com"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

AWSApplicationAutoscalingSageMakerEndpointPolicy es una [política AWS administrada](#) que: Política que otorga permisos a Application Auto Scaling para acceder SageMaker y CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de febrero de 2018 a las 19:58 UTC
- Hora de edición: 13 de noviembre de 2023 a las 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMaker",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationDiscoveryAgentAccess

AWSApplicationDiscoveryAgentAccess es una [política administrada por AWS](#) que: proporciona acceso al Agente Discovery para registrarse en Application Discovery Service de AWS.

Uso de la política

Puede asociar AWSApplicationDiscoveryAgentAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de mayo de 2016 a las 21:38 UTC
- Hora de edición: 24 de febrero de 2020 a las 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "arsenal:RegisterOnPremisesAgent"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

AWSApplicationDiscoveryAgentlessCollectorAccess es una [política administrada por AWS](#) que: permite a Application Discovery Service Agentless Collectors actualizarse, registrarse y comunicarse automáticamente con Application Discovery Service

Uso de la política

Puede asociar AWSApplicationDiscoveryAgentlessCollectorAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 16 de agosto de 2022 a las 21:00 UTC
- Hora de edición: 16 de agosto de 2022 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:DescribeImages"
      ],
      "Resource" : "arn:aws:ecr-public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    "Effect" : "Allow",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sts:GetServiceBearerToken"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationDiscoveryServiceFullAccess

AWSApplicationDiscoveryServiceFullAccess es una [política administrada por AWS](#) que: proporciona acceso total para ver y etiquetar los elementos de configuración mantenidos por AWS Application Discovery Service

Uso de la política

Puede asociar AWSApplicationDiscoveryServiceFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 11 de mayo de 2016 a las 21:30 UTC
- Hora de edición: 19 de junio de 2019 a las 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    }
  ]
}
```



```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "migrationhub.amazonaws.com",
        "dmsintegration.migrationhub.amazonaws.com",
        "smsintegration.migrationhub.amazonaws.com"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationAgentInstallationPolicy

`AWSApplicationMigrationAgentInstallationPolicy` es una [política administrada por AWS](#) que: permite instalar el Agente de replicación de AWS, que se utiliza con el Servicio de migración de aplicaciones de AWS (MGN) para migrar servidores externos a AWS. Asocie esta política a los usuarios o roles de IAM cuyas credenciales proporciona al instalar el Agente de replicación de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationAgentInstallationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de junio de 2022 a las 07:51 UTC
- Hora de edición: 20 de septiembre de 2022 a las 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",

```

```

    "mgn:RegisterAgentForMgn",
    "mgn:VerifyClientRoleForMgn"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "mgn:IssueClientCertificateForMgn"
  ],
  "Resource" : "arn:aws:mgn:*:*:source-server/*"
},
{
  "Effect" : "Allow",
  "Action" : "mgn:TagResource",
  "Resource" : "arn:aws:mgn:*:*:source-server/*",
  "Condition" : {
    "StringEquals" : {
      "mgn:CreateAction" : "RegisterAgentForMgn"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationAgentPolicy

AWSApplicationMigrationAgentPolicy es una [política administrada por AWS](#) permite instalar y usar el Agente de replicación de AWS, que se usa con el Servicio de migración de aplicaciones de AWS (MGN) para migrar servidores externos a AWS. Asocie esta política a los usuarios o roles de IAM cuyas credenciales proporciona al instalar el Agente de replicación de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationAgentPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de abril de 2021 a las 07:00 UTC
- Hora de edición: 20 de septiembre de 2022 a las 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",

```

```
    "mgn:UpdateAgentReplicationInfoForMgn",
    "mgn:UpdateAgentConversionInfoForMgn",
    "mgn:GetAgentInstallationAssetsForMgn",
    "mgn:GetAgentCommandForMgn",
    "mgn:GetAgentConfirmedResumeInfoForMgn",
    "mgn:GetAgentRuntimeConfigurationForMgn",
    "mgn:UpdateAgentBacklogForMgn",
    "mgn:GetAgentReplicationInfoForMgn"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "mgn:TagResource",
  "Resource" : "arn:aws:mgn:*:*:source-server/*"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationAgentPolicy_v2

AWSApplicationMigrationAgentPolicy_v2 es una [política administrada por AWS](#) que: permite usar el Agente de replicación de AWS, que se usa con el Servicio de migración de aplicaciones (MGN) de AWS para migrar los servidores externos de AWS. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSApplicationMigrationAgentPolicy_v2 a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de junio de 2022 a las 14:14 UTC
- Hora de edición: 6 de junio de 2022 a las 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationConversionServerPolicy

AWSApplicationMigrationConversionServerPolicy es una [política administrada por AWS](#) que: permite que el servidor de conversión del Servicio de migración de aplicaciones (MGN), que son instancias EC2 lanzadas por el Servicio de migración de aplicaciones, se comuniquen con el servicio MGN. Con esta política, MGN asocia un rol de IAM (como perfil de instancia EC2) a los servidores de conversión de MGN, que MGN lanza y termina automáticamente cuando es necesario. No es recomendable que asocie esta política a sus usuarios o roles de IAM. El Servicio de migración de aplicaciones utiliza los Servidores de conversión MGN cuando los usuarios eligen lanzar instancias de prueba o transición con la consola, la CLI o la API de MGN.

Uso de la política

Puede asociar AWSApplicationMigrationConversionServerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de abril de 2021 a las 06:48 UTC
- Hora de edición: 7 de abril de 2021 a las 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationEC2Access

AWSApplicationMigrationEC2Access es una [política administrada por AWS](#) que: proporciona las operaciones de Amazon EC2 necesarias para utilizar el Servicio de migración de aplicaciones (MGN) y así lanzar los servidores migrados como instancias de EC2. Asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar `AWSApplicationMigrationEC2Access` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de abril de 2021 a las 07:05 UTC
- Hora de edición: 6 de febrero de 2023 a las 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSnapshots",
      "ec2:DescribeImages",
      "ec2:DescribeVolumes"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "mgn.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2>DeleteLaunchTemplateVersions"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [

```

```
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "mgn.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "mgn.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:GetConsoleOutput",
      "ec2:GetConsoleScreenshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVolume"
    ],
  },
```

```
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateSecurityGroup",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template*"
  ],
  "Condition" : {
```

```
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:launch-template*"
    ],
    "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"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationFullAccess

AWSApplicationMigrationFullAccess es una [política administrada por AWS](#) que: concede permisos a todas las API públicas del Servicio de migración de aplicaciones (MGN) de AWS, así como permisos para leer la información clave del KMS. Asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSApplicationMigrationFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de abril de 2021 a las 06:56 UTC
- Hora de edición: 20 de abril de 2023 a las 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationMGHAccess

AWSApplicationMigrationMGHAccess es una [política administrada por AWS](#) que: permite que el Servicio de migración de aplicaciones (MGN) de AWS envíe metadatos sobre el progreso de los servidores que se migran mediante MGN a AWS Migration Hub (MGH). MGN crea automáticamente un rol de IAM con esta política asocia y lo adopta. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSApplicationMigrationMGHAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de abril de 2021 a las 07:10 UTC
- Hora de edición: 7 de abril de 2021 a las 07:10 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationReadOnlyAccess

AWSApplicationMigrationReadOnlyAccess es una [política administrada por AWS](#) que: proporciona permisos a todas las API públicas de solo lectura del Servicio de migración de aplicaciones (MGN), así como a algunas API de solo lectura de otros servicios de AWS que se requieren para poder aprovechar al máximo la consola MGN en modo de solo lectura. Asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSApplicationMigrationReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de abril de 2021 a las 07:15 UTC
- Hora de edición: 20 de marzo de 2023 a las 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "mgn:DescribeJobLogItems",
    "mgn:DescribeJobs",
    "mgn:DescribeSourceServers",
    "mgn:DescribeReplicationConfigurationTemplates",
    "mgn:GetLaunchConfiguration",
    "mgn:DescribeVcenterClients",
    "mgn:GetReplicationConfiguration",
    "mgn:DescribeLaunchConfigurationTemplates",
    "mgn:ListSourceServerActions",
    "mgn:ListTemplateActions",
    "mgn:ListApplications",
    "mgn:ListWaves",
    "mgn:ListExports",
    "mgn:ListImports",
    "mgn:ListImportErrors",
    "mgn:ListExportErrors"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicequotas:GetServiceQuota"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationReplicationServerPolicy

AWSApplicationMigrationReplicationServerPolicy es una [política administrada por AWS](#) que: permite que los servidores de replicación del Servicio de migración de aplicaciones (MGN), que son instancias EC2 lanzadas por el Servicio de migración de aplicaciones, se comuniquen con el servicio MGN y creen capturas de EBS en su interior. Cuenta de AWS Con esta política, el Servicio de migración de aplicaciones asigna un rol de IAM (como perfil de instancia EC2) a los Servidores de replicación de MGN, que MGN lanza y termina automáticamente, según sea necesario. Los Servidores de replicación MGN se utilizan para facilitar la replicación de datos desde sus servidores externos a AWS, como parte del proceso de migración gestionado mediante MGN. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSApplicationMigrationReplicationServerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de abril de 2021 a las 07:21 UTC
- Hora de edición: 7 de abril de 2021 a las 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",
        "mgn:NotifyAgentReplicationProgressForMgn",
        "mgn:NotifyAgentConnectedForMgn",
        "mgn:NotifyAgentDisconnectedForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
    }
  ]
}
```

```
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSnapshot"
      }
    }
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationServiceEc2InstancePolicy

AWSApplicationMigrationServiceEc2InstancePolicy es una [política administrada por AWS](#) que: permite instalar y usar el Agente de replicación de AWS, que utiliza el Servicio de migración de aplicaciones de AWS (MGN de AWS) para migrar los servidores de origen que se ejecutan en EC2 (entre regiones o entre zonas de disponibilidad). Con esta política, se debe asociar un rol de IAM (como un perfil de instancia de EC2) a las instancias de EC2.

Uso de la política

Puede asociar AWSApplicationMigrationServiceEc2InstancePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de agosto de 2023 a las 13:19 UTC
- Hora editada: 3 de enero de 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "mgn:RegisterAgentForMgn",
    "mgn:GetAgentInstallationAssetsForMgn"
  ],
  "Resource" : "*"
},
{
  "Sid" : "MgnAgentReplication",
  "Effect" : "Allow",
  "Action" : [
    "mgn:SendAgentMetricsForMgn",
    "mgn:SendAgentLogsForMgn",
    "mgn:UpdateAgentSourcePropertiesForMgn",
    "mgn:UpdateAgentReplicationInfoForMgn",
    "mgn:UpdateAgentConversionInfoForMgn",
    "mgn:GetAgentCommandForMgn",
    "mgn:GetAgentConfirmedResumeInfoForMgn",
    "mgn:GetAgentRuntimeConfigurationForMgn",
    "mgn:UpdateAgentBacklogForMgn",
    "mgn:GetAgentReplicationInfoForMgn"
  ],
  "Resource" : "arn:aws:mgn:*:*:source-server/*"
},
{
  "Sid" : "MgnSourceServerTagResource",
  "Effect" : "Allow",
  "Action" : "mgn:TagResource",
  "Resource" : "arn:aws:mgn:*:*:source-server/*",
  "Condition" : {
    "StringEquals" : {
      "mgn:CreateAction" : "RegisterAgentForMgn"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationServiceRolePolicy

AWSApplicationMigrationServiceRolePolicy es una [política administrada por AWS](#) que: permite que el Servicio de migración de aplicaciones de AWS cree y gestione los recursos AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de abril de 2021 a las 06:43 UTC
- Hora de edición: 20 de junio de 2023 a las 09:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```

    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "kms:ListRetirableGrants",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "mgh:AssociateCreatedArtifact",
      "mgh:CreateProgressUpdateStream",
      "mgh:DisassociateCreatedArtifact",
      "mgh:GetHomeRegion",
      "mgh:ImportMigrationTask",
      "mgh:NotifyMigrationTaskState",
      "mgh:PutResourceAttributes"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribeLaunchTemplates",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSubnets",
      "ec2:DescribeVolumes",
      "ec2:GetEbsDefaultKmsKeyId",
      "ec2:GetEbsEncryptionByDefault"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [

```

```
    "organizations:DescribeAccount"
  ],
  "Resource" : "arn:aws:organizations::*:account/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RegisterImage",
    "ec2:DeregisterImage"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplateVersion",
    "ec2:ModifyLaunchTemplate",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
```

```
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:GetConsoleOutput",
      "ec2:GetConsoleScreenshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "Null" : {
```

```
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
    }
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
```

```
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
```

```

    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
      "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2::*:launch-template/*",
      "arn:aws:ec2::*:security-group/*",
      "arn:aws:ec2::*:volume/*",
      "arn:aws:ec2::*:snapshot/*",
      "arn:aws:ec2::*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateLaunchTemplate",
          "CreateSecurityGroup",
          "CreateVolume",
          "CreateSnapshot",
          "RunInstances"
        ]
      }
    }
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationSSMAccess

AWSApplicationMigrationSSMAccess es una [política administrada por AWS](#) que: proporciona acceso a las operaciones de Amazon SSM necesarias para utilizar el Servicio de migración de aplicaciones (MGN) y así ejecutar documentos SSM personalizados tras la migración. Asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSApplicationMigrationSSMAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2022 a las 09:29 UTC
- Hora de edición: 20 de marzo de 2023 a las 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```

    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "mgn.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand",
      "ssm:DescribeDocument",
      "ssm:StartAutomationExecution"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/*",
      "arn:aws:ssm:*:*:automation-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/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSApplicationMigrationVCenterClientPolicy

AWSApplicationMigrationVCenterClientPolicy es una [política administrada por AWS](#) que: permite instalar y usar AWS VCenter Client, que se usa con el Servicio de migración de aplicaciones (MGN) de AWS para migrar servidores externos a AWS. Asocie esta política a los usuarios o roles de IAM cuyas credenciales proporciona al instalar AWS VCenter Client.

Uso de la política

Puede asociar `AWSApplicationMigrationVCenterClientPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de noviembre de 2021 a las 12:53 UTC
- Hora de edición: 8 de noviembre de 2021 a las 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",
        "mgn:SendVcenterClientMetricsForMgn",

```

```
        "mgn:DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
    ],
    "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppMeshEnvoyAccess

AWSAppMeshEnvoyAccess es una [política administrada por AWS](#) que: es una política de App Mesh Envoy que se usa para acceder a la configuración del nodo virtual.

Uso de la política

Puede asociar AWSAppMeshEnvoyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de julio de 2019 a las 21:29 UTC
- Hora de edición: 3 de julio de 2019 a las 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppMeshFullAccess

AWSAppMeshFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a las API de App Mesh de AWS y a la consola de administración.

Uso de la política

Puede asociar AWSAppMeshFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 16 de abril de 2019 a las 17:50 UTC
- Hora de edición: 7 de enero de 2021 a las 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStack*",
      "cloudformation:UpdateStack"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm:ListCertificates",
      "acm:DescribeCertificate",
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicediscovery:ListNamespaces",
      "servicediscovery:ListServices",
      "servicediscovery:ListInstances"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppMeshPreviewEnvoyAccess

AWSAppMeshPreviewEnvoyAccess es una [política administrada por AWS](#) que: es una política de App Mesh Preview Envoy que se usa para acceder a la configuración del nodo virtual.

Uso de la política

Puede asociar AWSAppMeshPreviewEnvoyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de agosto de 2019 a las 23:32 UTC
- Hora de edición: 5 de agosto de 2019 a las 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppMeshPreviewServiceRolePolicy

AWSAppMeshPreviewServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y los recursos utilizados o gestionados por App Mesh de AWS

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de junio de 2019 a las 19:07 UTC
- Hora de edición: 21 de agosto de 2019 a las 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppMeshReadOnly

AWSAppMeshReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a las API de App Mesh de AWS y a la consola de administración.

Uso de la política

Puede asociar AWSAppMeshReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 16 de abril de 2019 a las 17:51 UTC
- Hora de edición: 7 de enero de 2021 a las 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:Describe*",
        "appmesh:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
```

```
    "acm-pca:DescribeCertificateAuthority",
    "acm-pca:ListCertificateAuthorities"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:ListNamespaces",
    "servicediscovery:ListServices",
    "servicediscovery:ListInstances"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppMeshServiceRolePolicy

AWSAppMeshServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y los recursos utilizados o gestionados por AWS AppMesh

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 3 de junio de 2019 a las 18:30 UTC
- Hora de edición: 10 de octubre de 2023 a las 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppRunnerFullAccess

AWSAppRunnerFullAccess es una [política administrada por AWS](#) que: otorga permisos a todas las acciones de App Runner.

Uso de la política

Puede asociar AWSAppRunnerFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de enero de 2022 a las 04:02 UTC
- Hora de edición: 11 de enero de 2022 a las 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "iam:AWSServiceName" : "apprunner.amazonaws.com"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "iam:PassedToService" : "apprunner.amazonaws.com"
        }
    }
},
{
    "Sid" : "AppRunnerAdminAccess",
    "Effect" : "Allow",
    "Action" : "apprunner:*",
    "Resource" : "*"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppRunnerReadOnlyAccess

AWSAppRunnerReadOnlyAccess es una [política administrada por AWS](#) que: otorga permisos para publicar y ver detalles sobre los recursos de App Runner.

Uso de la política

Puede asociar AWSAppRunnerReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de febrero de 2022 a las 21:24 UTC
- Hora de edición: 24 de febrero de 2022 a las 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppRunnerServicePolicyForECRAccess

`AWSAppRunnerServicePolicyForECRAccess` es una [política administrada por AWS](#) que: es una política de servicio de AWS App Runner que otorga permisos de lectura a los recursos de Amazon ECR en la cuenta del cliente. Úsela en un rol que se transfiere a App Runner al crear o actualizar un servicio de App Runner.

Uso de la política

Puede asociar `AWSAppRunnerServicePolicyForECRAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de mayo de 2021 a las 19:17 UTC
- Hora de edición: 14 de mayo de 2021 a las 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Action" : [
  "ecr:GetDownloadUrlForLayer",
  "ecr:BatchGetImage",
  "ecr:DescribeImages",
  "ecr:GetAuthorizationToken",
  "ecr:BatchCheckLayerAvailability"
],
"Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppSyncAdministrator

`AWSAppSyncAdministrator` es una [política administrada por AWS](#) que: proporciona acceso administrativo al servicio AppSync, aunque no lo suficiente como para acceder a través de la consola.

Uso de la política

Puede asociar `AWSAppSyncAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de marzo de 2018 a las 21:20 UTC
- Hora de edición: 4 de noviembre de 2019 a las 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appsync.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/
AWSServiceRoleForAppSync*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppSyncInvokeFullAccess

AWSAppSyncInvokeFullAccess es una [política administrada por AWS](#) que: proporciona acceso de invocación total al servicio AppSync, tanto a través de la consola como de forma independiente

Uso de la política

Puede asociar AWSAppSyncInvokeFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de marzo de 2018 a las 21:21 UTC
- Hora de edición: 20 de marzo de 2018 a las 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppSyncPushToCloudWatchLogs

AWSAppSyncPushToCloudWatchLogs es una [política administrada por AWS](#) que: permite que AppSync envíe registros a la cuenta de CloudWatch del usuario.

Uso de la política

Puede asociar `AWSAppSyncPushToCloudWatchLogs` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2018 a las 19:38 UTC
- Hora de edición: 09 de abril de 2018 a las 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppSyncSchemaAuthor

AWSAppSyncSchemaAuthor es una [política administrada por AWS](#) que: brinda acceso para crear, actualizar y consultar schema.

Uso de la política

Puede asociar AWSAppSyncSchemaAuthor a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de marzo de 2018 a las 21:21 UTC
- Hora de edición: 1 de febrero de 2023 a las 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "appsync:GraphQL",
      "appsync:CreateResolver",
      "appsync:CreateType",
      "appsync>DeleteResolver",
      "appsync>DeleteType",
      "appsync:GetResolver",
      "appsync:GetType",
      "appsync:GetDataSource",
      "appsync:GetSchemaCreationStatus",
      "appsync:GetIntrospectionSchema",
      "appsync:GetGraphQLApi",
      "appsync:ListTypes",
      "appsync:ListApiKeys",
      "appsync:ListResolvers",
      "appsync:ListDataSources",
      "appsync:ListGraphQLApis",
      "appsync:StartSchemaCreation",
      "appsync:UpdateResolver",
      "appsync:UpdateType",
      "appsync:TagResource",
      "appsync:UntagResource",
      "appsync:ListTagsForResource",
      "appsync:CreateFunction",
      "appsync:UpdateFunction",
      "appsync:GetFunction",
      "appsync>DeleteFunction",
      "appsync:ListFunctions",
      "appsync:ListResolversByFunction",
      "appsync:EvaluateMappingTemplate",
      "appsync:EvaluateCode"
    ],
    "Resource" : "*"
  }
]
```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAppSyncServiceRolePolicy

AWSAppSyncServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los servicios y recursos de AWS utilizados o gestionados por AppSync

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de enero de 2020 a las 19:56 UTC
- Hora de edición: 21 de enero de 2020 a las 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingTargets",
      "xray:GetSamplingRules",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSArtifactAccountSync

AWSArtifactAccountSync es una [política administrada por AWS](#) que: concede a AWS Artifact acceso de solo lectura a las operaciones de AWSOrganizations.

Uso de la política

Puede asociar AWSArtifactAccountSync a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de abril de 2018 a las 23:04 UTC
- Hora de edición: 10 de abril de 2018 a las 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSArtifactReportsReadOnlyAccess

AWSArtifactReportsReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a los informes del servicio AWS Artifact.

Uso de la política

Puede asociar `AWSArtifactReportsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de enero de 2024 a las 22:42 UTC
- Hora editada: 2 de enero de 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSArtifactServiceRolePolicy

AWSArtifactServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Artifact recopile información sobre una organización a través del servicio AWS Organizations.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de agosto de 2023 a las 20:27 UTC
- Hora de edición: 21 de agosto de 2023 a las 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAuditManagerAdministratorAccess

AWSAuditManagerAdministratorAccess es una [política administrada por AWS](#) que: proporciona acceso administrativo para activar o desactivar AWS Audit Manager, actualizar la configuración y gestionar las evaluaciones, los controles y marcos

Uso de la política

Puede asociar AWSAuditManagerAdministratorAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de diciembre de 2020 a las 20:02 UTC
- Hora de edición: 30 de abril de 2022 a las 00:02 UTC

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

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",

```

```

    "organizations:DeregisterDelegatedAdministrator",
    "organizations:EnableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLikeIfExists" : {
      "organizations:ServicePrincipal" : [
        "auditmanager.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "IAMAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser",
    "iam:ListUsers",
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMAccessCreateSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "auditmanager.amazonaws.com"
    }
  }
},
{
  "Sid" : "IAMAccessManageSLR",
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteServiceLinkedRole",
    "iam:UpdateRoleDescription",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"

```



```
  },
  {
    "Sid" : "S3Access",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsCreateGrantAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "kms:GrantIsForAWSResource" : "true"
      },
      "StringLike" : {
        "kms:ViaService" : "auditmanager.*.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SNSAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : "*"
  },
  {
```

```
"Sid" : "CreateEventsAccess",
"Effect" : "Allow",
"Action" : [
  "events:PutRule"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "events:detail-type" : "Security Hub Findings - Imported"
  },
  "ForAllValues:StringEquals" : {
    "events:source" : [
      "aws.securityhub"
    ]
  }
}
},
{
  "Sid" : "EventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "events>DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events>ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
},
{
  "Sid" : "TagAccess",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAuditManagerServiceRolePolicy

AWSAuditManagerServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los recursos de Servicios de AWS utilizados o gestionados por AWS Audit Manager

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de diciembre de 2020 a las 15:12 UTC
- Hora editada: 6 de diciembre de 2023, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

AWSAutoScalingPlansEC2AutoScalingPolicy es una [política administrada por AWS](#) que: otorga permisos al escalado automático de AWS para pronosticar de forma habitual la capacidad, y generar acciones de escalado programadas para los grupos de escalado automático dentro de un plan de escalado

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de agosto de 2018 a las 22:46 UTC
- Hora de edición: 23 de agosto de 2018 a las 22:46 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupAuditAccess

AWSBackupAuditAccess es una [política administrada por AWS](#) que: otorga permisos a los usuarios para crear controles y marcos que definan sus expectativas para los recursos y actividades de Backup de AWS, y para auditar los recursos y las actividades de Backup de AWS con respecto a los controles y marcos definidos. Esta política otorga permisos a AWS Config y a servicios similares para que describan las expectativas de los usuarios y realicen auditorías. Esta política también otorga permisos para entregar informes de auditoría a S3 y servicios similares, y permite que los usuarios busquen y abran sus informes de auditoría.

Uso de la política

Puede asociar AWSBackupAuditAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de agosto de 2021 a las 01:02 UTC
- Hora de edición: 10 de abril de 2023 a las 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

        "backup:ListFrameworks",
        "backup:DescribeFramework",
        "backup>DeleteFramework",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup>CreateReportPlan",
        "backup:UpdateReportPlan",
        "backup:ListReportPlans",
        "backup:DescribeReportPlan",
        "backup>DeleteReportPlan",
        "backup:StartReportJob",
        "backup:ListReportJobs",
        "backup:DescribeReportJob"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeComplianceByConfigRule"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "config:GetComplianceDetailsByConfigRule"
    ],
    "Resource" : "arn:aws:config:*:*:config-rule/*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
    ],
    "Resource" : "arn:aws:s3:::*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupDataTransferAccess

`AWSBackupDataTransferAccess` es una [política administrada por AWS](#) que: permite que el Agente Backint de AWS complete la transferencia de datos de respaldo con el plano de almacenamiento de respaldo de AWS. Asocie esta política a los roles que asumen las instancias de EC2 que ejecutan SAP HANA con el agente Backint.

Uso de la política

Puede asociar `AWSBackupDataTransferAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de noviembre de 2022 a las 22:48 UTC
- Hora de edición: 10 de noviembre de 2022 a las 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:StartObject",
        "backup-storage:PutChunk",
        "backup-storage:GetChunk",
        "backup-storage:ListChunks",
        "backup-storage:ListObjects",
        "backup-storage:GetObjectMetadata",
        "backup-storage:NotifyObjectComplete"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupFullAccess

AWSBackupFullAccess es una [política administrada por AWS](#) que: está diseñada para los administradores de copia de seguridad. Otorga acceso total a las operaciones de copia de seguridad de AWS, incluida la creación o edición de planes de copia de seguridad, la asignación de recursos de AWS a planes de copia de seguridad, y la eliminación y restauración de copias de seguridad.

Uso de la política

Puede asociar `AWSBackupFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de noviembre de 2019 a las 22:21 UTC
- Hora editada: 27 de noviembre de 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Versión de la política

Versión de la política: v17 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```

    "rds:DescribeDBSnapshots",
    "rds:ListTagsForResource",
    "rds:DescribeDBInstances",
    "rds:describeDBEngineVersions",
    "rds:describeOptionGroups",
    "rds:describeOrderableDBInstanceOptions",
    "rds:describeDBSubnetGroups",
    "rds:describeDBClusterSnapshots",
    "rds:describeDBClusters",
    "rds:describeDBParameterGroups",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeDBClusterAutomatedBackups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RdsDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:DeleteDBSnapshot",
    "rds:DeleteDBClusterSnapshot"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "DynamoDbPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:ListBackups",
    "dynamodb:ListTables"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DynamoDbDeleteBackupPermissions",
  "Effect" : "Allow",

```

```

    "Action" : [
      "dynamodb:DeleteBackup"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "backup.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "EfsFileSystemPermissions",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:DescribeFilesystems"
    ],
    "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
  },
  {
    "Sid" : "Ec2Permissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSnapshots",
      "ec2:DescribeVolumes",
      "ec2:describeAvailabilityZones",
      "ec2:DescribeVpcs",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeImages",
      "ec2:DescribeSubnets",
      "ec2:DescribePlacementGroups",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeAddresses"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Ec2DeletePermissions",
    "Effect" : "Allow",
    "Action" : [

```



```

    "ec2:DeleteSnapshot",
    "ec2:DeregisterImage"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ResourceGroupTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetTagKeys",
    "tag:GetTagValues",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "StorageGatewayVolumePermissions",
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:DescribeCachediSCSIVolumes",
    "storagegateway:DescribeStorediSCSIVolumes"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
},
{
  "Sid" : "StorageGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:ListGateways"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:*"
},
{
  "Sid" : "StorageGatewayGatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:DescribeGatewayInformation",

```

```
    "storagegateway: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" : [
      "iam:GetResourceShareAssociations"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync es una [política administrada por AWS](#) que: otorga permiso a AWS BackupGateway para sincronizar los metadatos de las Máquinas virtuales en su nombre

Uso de la política

Puede asociar AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 15 de diciembre de 2022 a las 19:43 UTC
- Hora de edición: 15 de diciembre de 2022 a las 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "VMTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:TagResource",
        "backup-gateway:UntagResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupOperatorAccess

AWSBackupOperatorAccess es una [política administrada por AWS](#) que: otorga a los usuarios permisos para asignar recursos de AWS a los planes de respaldo, crear copias de seguridad a pedido y restaurar copias de seguridad. Esta política no permite que el usuario cree o edite planes de copia de seguridad o elimine copias de seguridad programadas una vez que están creadas.

Uso de la política

Puede asociar AWSBackupOperatorAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de noviembre de 2019 a las 22:23 UTC
- Hora de edición: 6 de septiembre de 2023 a las 20:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Versión de la política

Versión de la política: v15 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupOrganizationAdminAccess

AWSBackupOrganizationAdminAccess es una [política administrada por AWS](#) que: está diseñada para los administradores de copias de seguridad que utilizan la administración de copias de seguridad multicuenta para administrar las copias de seguridad de la organización.

Uso de la política

Puede asociar AWSBackupOrganizationAdminAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2020 a las 16:23 UTC
- Hora de edición: 18 de noviembre de 2022 a las 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisableAWSServiceAccess",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
```

```

    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "arn:aws:organizations::*:account/*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:AttachPolicy",
    "organizations:ListPoliciesForTarget",
    "organizations:ListTargetsForPolicy",
    "organizations:DetachPolicy",
    "organizations:DisablePolicyType",
    "organizations:DescribePolicy",
    "organizations:DescribeEffectivePolicy",
    "organizations:ListPolicies",
    "organizations:EnablePolicyType",
    "organizations:CreatePolicy",
    "organizations:UpdatePolicy",
    "organizations>DeletePolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLikeIfExists" : {
      "organizations:PolicyType" : [
        "BACKUP_POLICY"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccountsForParent",
    "organizations:ListAccounts",

```

```
    "organizations:DescribeOrganization",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListChildren",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganizationalUnit"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupRestoreAccessForSAPHANA

AWSBackupRestoreAccessForSAPHANA es una [política administrada por AWS](#) que: otorga permiso a Backup de AWS para restaurar una copia de seguridad de SAP HANA en Amazon EC2

Uso de la política

Puede asociar AWSBackupRestoreAccessForSAPHANA a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de noviembre de 2022 a las 22:43 UTC
- Hora de edición: 10 de noviembre de 2022 a las 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:RestoreDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupServiceLinkedRolePolicyForBackup

AWSBackupServiceLinkedRolePolicyForBackup es una [política administrada de AWS](#) que proporciona permiso a AWS Backup para crear copias de seguridad en su nombre en todos los servicios de AWS

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de junio de 2020 a las 23:08 UTC
- Hora editada: 15 de diciembre de 2023, 22:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Versión de la política

Versión de la política: v15 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    }
  ],
  {
```

```
"Sid" : "SnapshotCopyTagPermissions",
"Effect" : "Allow",
"Action" : "ec2:CreateTags",
"Resource" : "arn:aws:ec2:*::snapshot/*",
"Condition" : {
  "StringEquals" : {
    "ec2:CreateAction" : "CopySnapshot"
  }
}
},
{
  "Sid" : "EC2CreateBackupTagPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*::image/*",
    "arn:aws:ec2:*::snapshot/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AWSBackupManagedResource"
      ]
    }
  }
},
{
  "Sid" : "EC2CreateTagsPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*::image/*",
    "arn:aws:ec2:*::snapshot/*"
  ],
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSBackupManagedResource" : "false"
    }
  }
},
{
  "Sid" : "EC2RDSDescribePermissions",
  "Effect" : "Allow",
  "Action" : [
```



```

    "ec2:DescribeSnapshots",
    "ec2:DescribeSnapshotTierStatus",
    "ec2:DescribeImages",
    "rds:DescribeDBSnapshots",
    "rds:DescribeDBClusterSnapshots"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EBSCopyPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CopySnapshot",
  "Resource" : "arn:aws:ec2:*::snapshot/*"
},
{
  "Sid" : "EC2CopyPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CopyImage",
  "Resource" : "*"
},
{
  "Sid" : "EC2ModifyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeregisterImage",
    "ec2>DeleteSnapshot",
    "ec2:ModifySnapshotTier"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSBackupManagedResource" : "false"
    }
  }
},
{
  "Sid" : "RDSInstanceAndSnashotPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:AddTagsToResource",
    "rds:CopyDBSnapshot",
    "rds>DeleteDBSnapshot",
    "rds>DeleteDBInstanceAutomatedBackup"
  ],

```

```
    "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
  },
  {
    "Sid" : "RDSClusterPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:AddTagsToResource",
      "rds:CopyDBClusterSnapshot",
      "rds>DeleteDBClusterSnapshot"
    ],
    "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
  },
  {
    "Sid" : "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/*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

AWSBackupServiceLinkedRolePolicyForBackupTest es una [política administrada por AWS](#) que: proporciona permiso de Backup de AWS para crear copias de seguridad en su nombre en todos los servicios de AWS

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de mayo de 2020 a las 17:37 UTC
- Hora de edición: 12 de mayo de 2020 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Effect" : "Allow",
```

```
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
      }
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupServiceRolePolicyForBackup

AWSBackupServiceRolePolicyForBackup es una [política administrada de AWS](#) que proporciona permiso a AWS Backup para crear copias de seguridad en su nombre en todos los servicios de AWS

Uso de la política

Puede asociar AWSBackupServiceRolePolicyForBackup a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de enero de 2019 a las 21:01 UTC
- Hora editada: 15 de diciembre de 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Versión de la política

Versión de la política: v18 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb>DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",

```

```
    "rds:DescribeDBClusterSnapshots",
    "rds:CopyDBClusterSnapshot",
    "rds:DescribeDBClusterAutomatedBackups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "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" : "KMSEDataKeyEC2Permissions",
  "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:*:*:*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupServiceRolePolicyForRestores

AWSBackupServiceRolePolicyForRestores es una [política administrada por AWS](#) que: proporciona permiso de Backup de AWS para realizar restauraciones en su nombre en todos los servicios de AWS. Esta política incluye permisos para crear y eliminar recursos de AWS, como volúmenes de EBS, instancias de RDS y sistemas de archivos EFS, que forman parte del proceso de restauración.

Uso de la política

Puede asociar AWSBackupServiceRolePolicyForRestores a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de enero de 2019 a las 00:23 UTC
- Hora editada: 15 de diciembre de 2023, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Versión de la política

Versión de la política: v20 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "dynamodb:Scan",
  "dynamodb:Query",
  "dynamodb:UpdateItem",
  "dynamodb:PutItem",
  "dynamodb:GetItem",
  "dynamodb>DeleteItem",
  "dynamodb:BatchWriteItem",
  "dynamodb:DescribeTable"
],
"Resource" : "arn:aws:dynamodb:*:*:table/*"
},
{
  "Sid" : "DynamoDBBackupResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:RestoreTableFromBackup"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
},
{
  "Sid" : "EBSPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume",
    "ec2>DeleteVolume"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:volume/*"
  ]
},
{
  "Sid" : "EC2DescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots",
    "ec2:DescribeVolumes",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
```

```

    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSnapshotTierStatus"
  ],
  "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" : [
        "*"
    ]
}
]
}
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupServiceRolePolicyForS3Backup

AWSBackupServiceRolePolicyForS3Backup es una [política administrada por AWS](#) que: contiene los permisos necesarios para que el Backup de AWS haga copias de seguridad de los datos de cualquier bucket de S3. Esto incluye el acceso de lectura a todos los objetos de S3 y cualquier acceso de descifrado a todas las claves de KMS.

Uso de la política

Puede asociar `AWSBackupServiceRolePolicyForS3Backup` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de febrero de 2022 a las 17:40 UTC
- Hora de edición: 1 de septiembre de 2022 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBackupServiceRolePolicyForS3Restore

AWSBackupServiceRolePolicyForS3Restore es una [política administrada por AWS](#) que: contiene los permisos necesarios para que Backup de AWS restaure una copia de seguridad de S3 en un bucket. Esto incluye permisos de lectura y escritura para todos los buckets de S3, y permisos para GenerateDataKey y DescribeKey para todas las claves de KMS.

Uso de la política

Puede asociar AWSBackupServiceRolePolicyForS3Restore a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de febrero de 2022 a las 17:39 UTC

- Hora de edición: 7 de febrero de 2023 a las 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",

```

```

    "s3:PutObjectTagging",
    "s3:GetObjectAcl",
    "s3:PutObjectAcl",
    "s3:ListMultipartUploadParts",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "s3.*.amazonaws.com"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBatchFullAccess

AWSBatchFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a los recursos de Batch de AWS.

Uso de la política

Puede asociar `AWSBatchFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de diciembre de 2016 a las 19:35 UTC
- Hora de edición: 24 de octubre de 2022 a las 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeClusters",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",

```

```

    "eks:ListClusters",
    "logs:Describe*",
    "logs:Get*",
    "logs:TestMetricFilter",
    "logs:FilterLogEvents",
    "iam:ListInstanceProfiles",
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSBatchServiceRole",
    "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
    "arn:aws:iam::*:role/ecsInstanceRole",
    "arn:aws:iam::*:instance-profile/ecsInstanceRole",
    "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
    "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
    "arn:aws:iam::*:role/AWSBatchJobRole*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*Batch*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "batch.amazonaws.com"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBatchServiceEventTargetRole

AWSBatchServiceEventTargetRole es una [política administrada por AWS](#) que: habilita CloudWatch Event Target para el Envío de trabajos por lotes de AWS

Uso de la política

Puede asociar AWSBatchServiceEventTargetRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de febrero de 2018 a las 22:31 UTC
- Hora de edición: 28 de febrero de 2018 a las 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBatchServiceRole

AWSBatchServiceRole es una [política administrada por AWS](#) que: es una Política de rol de servicio por lote de AWS que permite el acceso a servicios relacionados, incluidos EC2, Autoscaling, EC2 Container service y los Registros de Cloudwatch.

Uso de la política

Puede asociar AWSBatchServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de diciembre de 2016 a las 19:36 UTC
- Hora editada: 5 de diciembre de 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Versión de la política

Versión de la política: v13 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:CreateLaunchTemplate",
        "ec2>DeleteLaunchTemplate",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
```



```
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:SetDesiredCapacity",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling:CreateOrUpdateTags",
    "autoscaling:SuspendProcesses",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "ecs:DescribeClusters",
    "ecs:DescribeContainerInstances",
    "ecs:DescribeTaskDefinition",
    "ecs:DescribeTasks",
    "ecs:ListAccountSettings",
    "ecs:ListClusters",
    "ecs:ListContainerInstances",
    "ecs:ListTaskDefinitionFamilies",
    "ecs:ListTaskDefinitions",
    "ecs:ListTasks",
    "ecs:CreateCluster",
    "ecs>DeleteCluster",
    "ecs:RegisterTaskDefinition",
    "ecs:DeregisterTaskDefinition",
    "ecs:RunTask",
    "ecs:StartTask",
    "ecs:StopTask",
    "ecs:UpdateContainerAgent",
    "ecs:DeregisterContainerInstance",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogGroups",
    "iam:GetInstanceProfile",
    "iam:GetRole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSBatchPolicyStatement2",
  "Effect" : "Allow",
  "Action" : "ecs:TagResource",
```

```
    "Resource" : [
      "arn:aws:ecs:*:*:task/*_Batch_*"
    ]
  },
  {
    "Sid" : "AWSBatchPolicyStatement3",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn",
          "ecs-tasks.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement4",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "spot.amazonaws.com",
          "spotfleet.amazonaws.com",
          "autoscaling.amazonaws.com",
          "ecs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement5",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
```

```
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ec2:CreateAction" : "RunInstances"
        }
    }
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBillingConductorFullAccess

AWSBillingConductorFullAccess es una [política administrada AWS](#) que: utiliza la política administrada de AWSBillingConductorFullAccess para permitir el acceso total a la consola (ABC) y a las API de AWS Billing Conductor. Esta política permite a los usuarios enumerar, crear y eliminar los recursos de ABC.

Uso de la política

Puede asociar AWSBillingConductorFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de abril de 2022 a las 18:02 UTC
- Hora de edición: 13 de abril de 2022 a las 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBillingConductorReadOnlyAccess

`AWSBillingConductorReadOnlyAccess` es una [política administrada AWS](#) que: utiliza la política administrada de `AWSBillingConductorReadOnlyAccess` para permitir el acceso de solo lectura a la

consola de AWS Billing Conductor (ABC) y a las API. Esta política concede el permiso para obtener y enumerar todos los recursos de IAM. No incluye la capacidad de crear o eliminar recursos.

Uso de la política

Puede asociar `AWSBillingConductorReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de abril de 2022 a las 18:02 UTC
- Hora de edición: 13 de abril de 2022 a las 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBillingReadOnlyAccess

AWSBillingReadOnlyAccess es una [política administrada por AWS](#) que: permite a los usuarios ver las facturas en la Consola de facturación.

Uso de la política

Puede asociar AWSBillingReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de agosto de 2020 a las 20:08 UTC
- Hora editada: 17 de enero de 2024, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Sid" : "VisualEditor0",
    "Effect" : "Allow",
    "Action" : [
      "account:GetAccountInformation",
      "aws-portal:ViewBilling",
      "billing:GetBillingData",
      "billing:GetBillingDetails",
      "billing:GetBillingNotifications",
      "billing:GetBillingPreferences",
      "billing:GetCredits",
      "billing:GetContractInformation",
      "billing:GetIAMAccessPreference",
      "billing:GetSellerOfRecord",
      "billing:ListBillingViews",
      "budgets:ViewBudget",
      "budgets:DescribeBudgetActionsForBudget",
      "budgets:DescribeBudgetAction",
      "budgets:DescribeBudgetActionsForAccount",
      "budgets:DescribeBudgetActionHistories",
      "ce:DescribeCostCategoryDefinition",
      "ce:GetCostAndUsage",
      "ce:ListCostCategoryDefinitions",
      "ce:ListTagsForResource",
      "ce:ListCostAllocationTags",
      "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" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM es una [política administrada AWS](#) que: otorga permisos para controlar los recursos de AWS. Por ejemplo, inicia y detiene las instancias de Amazon EC2 o Amazon RDS mediante la ejecución de los scripts de AWS Systems Manager (SSM).

Uso de la política

Puede asociar AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de mayo de 2022 a las 19:03 UTC
- Hora de edición: 25 de mayo de 2022 a las 19:03 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",

```

```
    "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
    "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
    "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBudgetsActionsWithAWSResourceControlAccess

`AWSBudgetsActionsWithAWSResourceControlAccess` es una [política administrada por AWS](#) que: concede acceso total a las Acciones presupuestarias de AWS, incluido el uso de las Acciones presupuestarias para controlar el estado de los recursos de AWS en funcionamiento mediante la AWS Management Console

Uso de la política

Puede asociar `AWSBudgetsActionsWithAWSResourceControlAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de octubre de 2020 a las 17:19 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
```

```
    "ec2:DescribeInstances",
    "iam:ListGroups",
    "iam:ListPolicies",
    "iam:ListRoles",
    "iam:ListUsers",
    "organizations:ListAccounts",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListPolicies",
    "organizations:ListRoots",
    "rds:DescribeDBInstances",
    "sns:ListTopics"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBudgetsReadOnlyAccess

AWSBudgetsReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a la Consola de presupuestos de AWS a través de la AWS Management Console.

Uso de la política

Puede asociar AWSBudgetsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 15 de octubre de 2020 a las 17:18 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBugBustFullAccess

`AWSBugBustFullAccess` es una [política administrada por AWS](#) que: es una política de IAM que concede a los usuarios acceso total a la consola BugBust de AWS

Uso de la política

Puede asociar `AWSBugBustFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2021 a las 07:03 UTC
- Hora de edición: 22 de julio de 2021 a las 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

```

    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "bugbust.amazonaws.com"
        }
      }
    }
  ]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBugBustPlayerAccess

AWSBugBustPlayerAccess es una [política administrada por AWS](#) que: es una política de IAM que concede a los usuarios acceso para participar en los eventos de BugBust de AWS

Uso de la política

Puede asociar AWSBugBustPlayerAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2021 a las 07:15 UTC
- Hora de edición: 24 de junio de 2021 a las 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
      "Resource" : "*"
    },
    {
```



```
    "Sid" : "CodeGuruProfilerPermission",
    "Effect" : "Allow",
    "Action" : [
      "codeguru-profiler:DescribeProfilingGroup"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSBugBustPlayerAccess",
    "Effect" : "Allow",
    "Action" : [
      "bugbust:ListBugs",
      "bugbust:ListProfilingGroups",
      "bugbust:JoinEvent",
      "bugbust:GetEvent",
      "bugbust:ListEvents",
      "bugbust:GetJoinEventStatus",
      "bugbust:ListEventScores",
      "bugbust:ListEventParticipants",
      "bugbust:UpdateWorkItem",
      "bugbust:ListPullRequests"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSBugBustServiceRolePolicy

AWSBugBustServiceRolePolicy es una [política administrada por AWS](#) que: otorga permisos a BugBust de AWS para acceder a los recursos en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de junio de 2021 a las 06:59 UTC
- Hora de edición: 24 de junio de 2021 a las 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

```
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a AWS Certificate Manager (ACM)

Uso de la política

Puede asociar AWSCertificateManagerFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de enero de 2016 a las 17:02 UTC
- Hora de edición: 17 de agosto de 2020 a las 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "acm:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "acm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus",
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCertificateManagerPrivateCAAuditor

AWSCertificateManagerPrivateCAAuditor es una [política administrada AWS](#) que: proporciona a los auditores acceso a AWS Certificate Manager Private Certificate Authority

Uso de la política

Puede asociar AWSCertificateManagerPrivateCAAuditor a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de octubre de 2018 a las 16:51 UTC
- Hora de edición: 17 de agosto de 2020 a las 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",

```

```
    "acm-pca:ListTags"
  ],
  "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "acm-pca:ListCertificateAuthorities"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCertificateManagerPrivateCAFullAccess

AWSCertificateManagerPrivateCAFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS Certificate Manager Private Certificate Authority

Uso de la política

Puede asociar AWSCertificateManagerPrivateCAFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de octubre de 2018 a las 16:54 UTC
- Hora de edición: 23 de octubre de 2018 a las 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCertificateManagerPrivateCAPrivilegedUser

AWSCertificateManagerPrivateCAPrivilegedUser es una [política administrada AWS](#) que: proporciona a los usuarios de certificados con privilegios acceso a AWS Certificate Manager Private Certificate Authority

Uso de la política

Puede asociar `AWSCertificateManagerPrivateCAPrivilegedUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de junio de 2019 a las 17:43 UTC
- Hora de edición: 20 de junio de 2019 a las 17:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCertificateManagerPrivateCAReadOnly

AWSCertificateManagerPrivateCAReadOnly es una [política administrada por AWS](#) que proporciona acceso de solo lectura a AWS Certificate Manager Private Certificate Authority

Uso de la política

Puede asociar AWSCertificateManagerPrivateCAReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de octubre de 2018 a las 16:57 UTC
- Hora de edición: 17 de agosto de 2020 a las 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
    ]
  }
}
```

```
    "acm-pca:ListPermissions",
    "acm-pca:ListTags"
  ],
  "Resource" : "*"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCertificateManagerPrivateCAUser

AWSCertificateManagerPrivateCAUser es una [política administrada por AWS](#) que: proporciona a los usuarios de certificados acceso a AWS Certificate Manager Private Certificate Authority

Uso de la política

Puede asociar `AWSCertificateManagerPrivateCAUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de octubre de 2018 a las 16:53 UTC
- Hora de edición: 20 de junio de 2019 a las 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCertificateManagerReadOnly

AWSCertificateManagerReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AWS Certificate Manager (ACM).

Uso de la política

Puede asociar AWSCertificateManagerReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de enero de 2016 a las 17:07 UTC
- Hora de edición: 15 de marzo de 2021 a las 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSChatbotServiceLinkedRolePolicy

AWSChatbotServiceLinkedRolePolicy es una [política administrada por AWS](#) que otorga el rol vinculado a un servicio utilizado por AWS Chatbot.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2019 a las 16:39 UTC
- Hora de edición: 18 de noviembre de 2019 a las 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Unsubscribe",
        "sns:Subscribe",
        "sns:ListSubscriptions"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : [
      "logs:PutLogEvents",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:CreateLogGroup",
      "logs:DescribeLogGroups"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/chatbot/*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCleanRoomsFullAccess

AWSCleanRoomsFullAccesses una [política AWS gestionada](#) que: permite el acceso total a los recursos de las salas AWS limpias y el acceso a los relacionados Servicios de AWS.

Uso de la política

Puede asociar AWSCleanRoomsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de enero de 2023 a las 16:10 UTC
- Hora editada: 21 de marzo de 2024 a las 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
```

```

    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
},
{
  "Sid" : "ListPoliciesToInspectServiceRolePolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListPolicies"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetPolicyToInspectServiceRolePolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
  ],
  "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
},
{
  "Sid" : "ConsoleDisplayTables",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:GetSchema",
    "glue:GetSchemaVersion",
    "glue:BatchGetPartition"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsolePickQueryResultsBucketListAll",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],

```

```
    "Resource" : "*"
  },
  {
    "Sid" : "SetQueryResultsBucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucketVersions"
    ],
    "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
  },
  {
    "Sid" : "WriteQueryResults",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleDisplayQueryResults",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
  },
  {
    "Sid" : "EstablishLogDeliveries",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs:GetLogDelivery",
      "logs:UpdateLogDelivery",
      "logs>DeleteLogDelivery",
      "logs:ListLogDeliveries"
    ],
    "Resource" : "*",
```

```
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : "cleanrooms.amazonaws.com"
  }
},
{
  "Sid" : "SetupLogGroupsDescribe",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
  }
},
{
  "Sid" : "SetupLogGroupsCreate",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
  }
},
{
  "Sid" : "SetupLogGroupsResourcePolicy",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeResourcePolicies",
    "logs:PutResourcePolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "ConsoleLogSummaryQueryLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
    "Sid" : "ConsoleLogSummaryObtainLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:GetQueryResults"
    ],
    "Resource" : "*"
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSCleanRoomsFullAccessNoQuerying

`AWSCleanRoomsFullAccessNoQuerying` es una [política administrada por AWS](#) que: permite el acceso total a los recursos de las salas limpias de AWS, excepto las consultas en una colaboración y el acceso a los Servicios de AWS relacionados.

Uso de la política

Puede asociar `AWSCleanRoomsFullAccessNoQuerying` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de enero de 2023 a las 16:12 UTC
- Hora de edición: 31 de julio de 2023 a las 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCleanRoomsMLFullAccess

AWSCleanRoomsMLFullAccesses una [política AWS gestionada](#) que: permite el acceso total a los recursos de aprendizaje automático de salas AWS limpias y el acceso a los relacionados Servicios de AWS.

Uso de la política

Puede asociar AWSCleanRoomsMLFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2023 a las 21:02 UTC
- Hora editada: 29 de noviembre de 2023 a las 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms: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*"
}
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCleanRoomsMLReadOnlyAccess

AWSCleanRoomsMLReadOnlyAccesses una [política AWS gestionada](#) que: permite el acceso de solo lectura a los recursos de aprendizaje automático de salas AWS limpias y el acceso de solo lectura a los recursos de salas limpias relacionados AWS

Uso de la política

Puede asociar `AWSCleanRoomsMLReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2023 a las 20:55 UTC
- Hora editada: 29 de noviembre de 2023 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",

```



```
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CleanRoomsMLRead",
    "Effect" : "Allow",
    "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCleanRoomsReadOnlyAccess

AWSCleanRoomsReadOnlyAccess es una [política administrada por AWS](#) que: permite el acceso de solo lectura a los recursos de las Salas limpias de AWS y el acceso de solo lectura a los recursos relacionados de AWS Glue y los Registros de Amazon CloudWatch.

Uso de la política

Puede asociar AWSCleanRoomsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 12 de enero de 2023 a las 16:10 UTC
- Hora de edición: 12 de enero de 2023 a las 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGet*",
        "cleanrooms:Get*",
        "cleanrooms:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleLogSummaryQueryLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
    "Sid" : "ConsoleLogSummaryObtainLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:GetQueryResults"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloud9Administrator

AWSCloud9Administrator es una [política administrada por AWS](#) que: proporciona acceso de administrador a Cloud9 de AWS.

Uso de la política

Puede asociar AWSCloud9Administrator a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2017 a las 16:17 UTC
- Hora de edición: 11 de octubre de 2023 a las 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
    "StringLike" : {
      "iam:AWSServiceName" : "cloud9.amazonaws.com"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession",
      "ssm:GetConnectionStatus"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ssm:resourceTag/aws:cloud9:environment" : "*"
      },
      "StringEquals" : {
        "aws:CalledViaFirst" : "cloud9.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloud9EnvironmentMember

AWSCloud9EnvironmentMember es una [política administrada por AWS](#) que: ofrece la posibilidad de recibir una invitación para los entornos de desarrollo compartidos de Cloud9 de AWS.

Uso de la política

Puede asociar AWSCloud9EnvironmentMember a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2017 a las 16:18 UTC
- Hora de edición: 11 de octubre de 2023 a las 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloud9ServiceRolePolicy

AWSCloud9ServiceRolePolicy es una [política administrada por AWS](#) que: es una Política de roles vinculados a un servicio para AWS Cloud9

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2017 a las 13:44 UTC
- Hora de edición: 17 de enero de 2022 a las 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:CreateSecurityGroup",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "cloudformation:CreateStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResources"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2>DeleteSecurityGroup",
      "ec2:AuthorizeSecurityGroupIngress"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation>DeleteStack"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  }
]
```

```
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/Name" : "aws-cloud9-*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:StartInstances",
      "ec2:StopInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:StartInstances",
      "ec2:StopInstances"
    ],
    "Resource" : [
      "arn:aws:license-manager:*:*:license-configuration:*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:GetInstanceProfile"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:instance-profile/cloud9/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
  },
```

```
    "Resource" : [
      "arn:aws:iam::*:role/service-role/AWSCloud9SSMAccessRole"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloud9SSMInstanceProfile

AWSCloud9SSMInstanceProfile es una [política administrada por AWS](#) que: se utilizará para asociar un rol a un InstanceProfile que permitirá a Cloud9 usar el administrador de sesiones SSM para conectarse a la instancia

Uso de la política

Puede asociar AWSCloud9SSMInstanceProfile a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de mayo de 2020 a las 11:40 UTC
- Hora de edición: 14 de mayo de 2020 a las 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloud9User

AWSCloud9User es una [política administrada por AWS](#) que: concede permisos para crear entornos de desarrollo de AWS Cloud9 y administrar entornos propios.

Uso de la política

Puede asociar `AWSCloud9User` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2017 a las 16:16 UTC
- Hora de edición: 11 de octubre de 2023 a las 13:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudFormationFullAccess

AWSCloudFormationFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS CloudFormation.

Uso de la política

Puede asociar AWSCloudFormationFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de julio de 2019 a las 21:50 UTC
- Hora de edición: 26 de julio de 2019 a las 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudFormationReadOnlyAccess

AWSCloudFormationReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso a AWS CloudFormation a través de la AWS Management Console.

Uso de la política

Puede asociar AWSCloudFormationReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 13 de noviembre de 2019 a las 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudFrontLogger

AWSCloudFrontLogger es una [política administrada por AWS](#) que: concede a CloudFront Logger permisos de escritura en los Registros de CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de junio de 2018 a las 20:15 UTC
- Hora de edición: 22 de noviembre de 2019 a las 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudHSMFullAccess

AWSCloudHSMFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todos los recursos de CloudHSM.

Uso de la política

Puede asociar AWSCloudHSMFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudHSMReadOnlyAccess

AWSCloudHSMReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a todos los recursos de CloudHSM.

Uso de la política

Puede asociar AWSCloudHSMReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudHSMRole

AWSCloudHSMRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio de AWS CloudHSM.

Uso de la política

Puede asociar AWSCloudHSMRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudMapDiscoverInstanceAccess

AWSCloudMapDiscoverInstanceAccess es una [política administrada por AWS](#) que: proporciona acceso a la API de descubrimiento de mapas de Nube de AWS.

Uso de la política

Puede asociar AWSCloudMapDiscoverInstanceAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2018 a las 00:02 UTC
- Hora de edición: 20 de septiembre de 2023 a las 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudMapFullAccess

AWSCloudMapFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todas las acciones del mapa de Nube de AWS.

Uso de la política

Puede asociar AWSCloudMapFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2018 a las 23:57 UTC
- Hora de edición: 29 de julio de 2020 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53>DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudMapReadOnlyAccess

AWSCloudMapReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a todas las acciones del mapa de Nube de AWS.

Uso de la política

Puede asociar AWSCloudMapReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de noviembre de 2018 a las 23:45 UTC
- Hora de edición: 20 de septiembre de 2023 a las 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    ]
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudMapRegisterInstanceAccess

AWSCloudMapRegisterInstanceAccess es una [política administrada por AWS](#) que: proporciona acceso a nivel de registrante a las acciones de Mapas de Nube de AWS.

Uso de la política

Puede asociar AWSCloudMapRegisterInstanceAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2018 a las 00:04 UTC
- Hora de edición: 20 de septiembre de 2023 a las 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudShellFullAccess

AWSCloudShellFullAccess es una [política administrada por AWS](#) que: permite utilizar CloudShell de AWS con todas las características

Uso de la política

Puede asociar AWSCloudShellFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 18:07 UTC
- Hora de edición: 15 de diciembre de 2020 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudTrail_FullAccess

AWSCloudTrail_FullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS CloudTrail.

Uso de la política

Puede asociar AWSCloudTrail_FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de octubre de 2020 a las 23:41 UTC
- Hora de edición: 22 de febrero de 2021 a las 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:AddPermission",
      "sns:CreateTopic",
      "sns:SetTopicAttributes",
      "sns:GetTopicAttributes"
    ],
    "Resource" : [
      "arn:aws:sns:*:*:aws-cloudtrail-logs*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-cloudtrail-logs*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation",
      "s3:GetBucketPolicy"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudtrail:*",
    "Resource" : "*"
  }
]
```



```
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles",
    "iam:GetRolePolicy",
    "iam:GetUser"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "cloudtrail.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateKey",
    "kms:CreateAlias",
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
    "lambda:ListFunctions"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudTrail_ReadOnlyAccess

AWSCloudTrail_ReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AWS CloudTrail.

Uso de la política

Puede asociar AWSCloudTrail_ReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de junio de 2022 a las 17:19 UTC
- Hora de edición: 14 de junio de 2022 a las 17:19 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy es una [política administrada por AWS](#) que: utiliza el rol vinculado al servicio denominado AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents. CloudWatch utiliza este rol vinculado al servicio para realizar acciones de la administración de incidentes de AWS System Manager, cuando una alarma de CloudWatch pasa al estado de ALARMA. Esta política otorga permiso para iniciar incidentes en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de abril de 2021 a las 13:30 UTC
- Hora de edición: 27 de abril de 2021 a las 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
```

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeArtifactAdminAccess

AWSCodeArtifactAdminAccess es una [política administrada por AWS](#) que: brinda acceso total a CodeArtifact de AWS a través de la AWS Management Console.

Uso de la política

Puede asociar AWSCodeArtifactAdminAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 16 de junio de 2020 a las 23:53 UTC
- Hora de edición: 16 de junio de 2020 a las 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "codeartifact:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "sts:GetServiceBearerToken",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "sts:AWSServiceName" : "codeartifact.amazonaws.com"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeArtifactReadOnlyAccess

AWSCodeArtifactReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a CodeArtifact de AWS a través de la AWS Management Console.

Uso de la política

Puede asociar AWSCodeArtifactReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de junio de 2020 a las 21:23 UTC
- Hora de edición: 25 de junio de 2020 a las 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codeartifact:ReadFromRepository"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeBuildAdminAccess

AWSCodeBuildAdminAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS CodeBuild a través de la AWS Management Console. Asocie también Amazon3ReadOnlyAccess para proporcionar acceso a la descarga de artefactos de compilación, y asocie lamFullAccess para crear y administrar el rol de servicio de CodeBuild.

Uso de la política

Puede asociar AWSCodeBuildAdminAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2016 a las 19:04 UTC
- Hora de edición: 31 de julio de 2023 a las 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Versión de la política

Versión de la política: v13 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events>DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs>DeleteLogGroup"
      ],
      "Effect" : "Allow",
    }
  ]
}
```

```

    "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
  },
  {
    "Sid" : "SSMParameterWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
  },
  {
    "Sid" : "SSMStartSessionAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : "arn:aws:ecs:*:*:task/*/*"
  },
  {
    "Sid" : "CodeStarConnectionsReadWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:CreateConnection",
      "codestar-connections>DeleteConnection",
      "codestar-connections:UpdateConnectionInstallation",
      "codestar-connections:TagResource",
      "codestar-connections:UntagResource",
      "codestar-connections:ListConnections",
      "codestar-connections:ListInstallationTargets",
      "codestar-connections:ListTagsForResource",
      "codestar-connections:GetConnection",
      "codestar-connections:GetIndividualAccessToken",
      "codestar-connections:GetInstallationUrl",
      "codestar-connections:PassConnection",
      "codestar-connections:StartOAuthHandshake",
      "codestar-connections:UseConnection"
    ],
    "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
  },
  {
    "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" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeBuildDeveloperAccess

AWSCodeBuildDeveloperAccess es una [política administrada por AWS](#) que: proporciona acceso a AWS CodeBuild a través de la AWS Management Console, pero no permite la administración del proyecto de CodeBuild. Asocie también AmazonS3ReadOnlyAccess para permitir el acceso a la descarga de artefactos de construcción.

Uso de la política

Puede asociar AWSCodeBuildDeveloperAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2016 a las 19:02 UTC
- Hora de edición: 31 de julio de 2023 a las 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
```

```
    "Effect" : "Allow",
    "Action" : [
      "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
  },
  {
    "Sid" : "SSMStartSessionAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : "arn:aws:ecs:*:*:task/*/*"
  },
  {
    "Sid" : "CodeStarConnectionsUserAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:ListConnections",
      "codestar-connections:GetConnection"
    ],
    "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
  },
  {
    "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"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeBuildReadOnlyAccess

AWSCodeBuildReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AWS CodeBuild a través de la AWS Management Console. Asocie también [Amazons3ReadOnlyAccess](#) para permitir el acceso a la descarga de artefactos de construcción.

Uso de la política

Puede asociar AWSCodeBuildReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2016 a las 19:03 UTC
- Hora de edición: 14 de septiembre de 2020 a las 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeCommitFullAccess

AWSCodeCommitFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS CodeCommit a través de AWS Management Console.

Uso de la política

Puede asociar AWSCodeCommitFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de julio de 2015 a las 17:02 UTC
- Hora de edición: 17 de julio de 2023 a las 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "codecommit:*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
    "Effect" : "Allow",
    "Action" : [
      "events:DeleteRule",
      "events:DescribeRule",
      "events:DisableRule",
      "events:EnableRule",
      "events:PutRule",
      "events:PutTargets",
      "events:RemoveTargets",
      "events:ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/codecommit*"
  },
  {
    "Sid" : "SNSTopicAndSubscriptionAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns>DeleteTopic",
      "sns:Subscribe",
      "sns:Unsubscribe",
      "sns:SetTopicAttributes"
    ],
    "Resource" : "arn:aws:sns:*:*:codecommit*"
  },
  {
    "Sid" : "SNSTopicAndSubscriptionReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics",
      "sns:ListSubscriptionsByTopic",
      "sns:GetTopicAttributes"
    ],
    "Resource" : "*"
  }
]
```

```
},
{
  "Sid" : "LambdaReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:ListFunctions"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListUsers"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyConsoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListAccessKeys",
    "iam:ListSSHPublicKeys",
    "iam:ListServiceSpecificCredentials"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "IAMUserSSHKeys",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteSSHPublicKey",
    "iam:GetSSHPublicKey",
    "iam:ListSSHPublicKeys",
    "iam:UpdateSSHPublicKey",
    "iam:UploadSSHPublicKey"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "IAMSelfManageServiceSpecificCredentials",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceSpecificCredential",
```

```

    "iam:UpdateServiceSpecificCredential",
    "iam>DeleteServiceSpecificCredential",
    "iam:ResetServiceSpecificCredential"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "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/*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeCommitPowerUser

AWSCodeCommitPowerUser es una [política administrada por AWS](#) que: proporciona acceso total a los repositorios de AWS CodeCommit, pero no permite su eliminación.

Uso de la política

Puede asociar AWSCodeCommitPowerUser a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 9 de julio de 2015 a las 17:06 UTC
- Hora de edición: 17 de julio de 2023 a las 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Versión de la política

Versión de la política: v15 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit>DeleteBranch",
        "codecommit>DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
      ]
    }
  ]
}
```



```
    "codecommit:GitPull",
    "codecommit:GitPush"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:DisableRule",
    "events:EnableRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/codecommit*"
},
{
  "Sid" : "SNSTopicAndSubscriptionAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:codecommit*"
},
{
  "Sid" : "SNSTopicAndSubscriptionReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "sns:GetTopicAttributes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LambdaReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:ListFunctions"
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyListAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListUsers"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyConsoleAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListAccessKeys",
      "iam:ListSSHPublicKeys",
      "iam:ListServiceSpecificCredentials"
    ],
    "Resource" : "arn:aws:iam::*:user/${aws:username}"
  },
  {
    "Sid" : "IAMUserSSHKeys",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteSSHPublicKey",
      "iam:GetSSHPublicKey",
      "iam:ListSSHPublicKeys",
      "iam:UpdateSSHPublicKey",
      "iam:UploadSSHPublicKey"
    ],
    "Resource" : "arn:aws:iam::*:user/${aws:username}"
  },
  {
    "Sid" : "IAMSelfManageServiceSpecificCredentials",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceSpecificCredential",
      "iam:UpdateServiceSpecificCredential",
      "iam>DeleteServiceSpecificCredential",
      "iam:ResetServiceSpecificCredential"
    ],
    "Resource" : "arn:aws:iam::*:user/${aws:username}"
  },
  },
```

```
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "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/*"
  }
]

```

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeCommitReadOnly

AWSCodeCommitReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AWS CodeCommit a través de la AWS Management Console.

Uso de la política

Puede asociar AWSCodeCommitReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de julio de 2015 a las 17:05 UTC
- Hora de edición: 18 de agosto de 2021 a las 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
    }
  ]
}
```

```

    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyListAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListUsers"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMReadOnlyConsoleAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListSSHPublicKeys",
      "iam:ListServiceSpecificCredentials",
      "iam:ListAccessKeys",
      "iam:GetSSHPublicKey"
    ],
    "Resource" : "arn:aws:iam::*:user/${aws:username}"
  },
  {
    "Sid" : "CodeStarConnectionsReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:ListConnections",
      "codestar-connections:GetConnection"
    ],
    "Resource" : "arn:aws:codestar-connections::*:connection/*"
  },
  {
    "Sid" : "CodeStarNotificationsReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:DescribeNotificationRule"
    ],
    "Resource" : "*",
    "Condition" : {
      "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" : "*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployDeployerAccess

AWSCodeDeployDeployerAccess es una [política administrada por AWS](#) que: proporciona acceso para registrar e implementar una revisión.

Uso de la política

Puede asociar AWSCodeDeployDeployerAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de mayo de 2015 a las 18:18 UTC
- Hora de edición: 2 de abril de 2020 a las 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ]
    }
  ]
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployFullAccess

AWSCodeDeployFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a los recursos de CodeDeploy.

Uso de la política

Puede asociar AWSCodeDeployFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de mayo de 2015 a las 18:13 UTC
- Hora de edición: 2 de abril de 2020 a las 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
  },
  {
    "Sid" : "CodeStarNotificationsReadWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:CreateNotificationRule",
      "codestar-notifications:DescribeNotificationRule",
      "codestar-notifications:UpdateNotificationRule",
      "codestar-notifications>DeleteNotificationRule",
      "codestar-notifications:Subscribe",
      "codestar-notifications:Unsubscribe"
    ],
    "Resource" : "*",
    "Condition" : {
      "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" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployReadOnlyAccess

AWSCodeDeployReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a los recursos de CodeDeploy.

Uso de la política

Puede asociar AWSCodeDeployReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de mayo de 2015 a las 18:21 UTC
- Hora de edición: 2 de abril de 2020 a las 16:20 UTC

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

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
```

```
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployRole

AWSCodeDeployRole es una [política administrada AWS](#) que: proporciona acceso al servicio CodeDeploy para expandir las etiquetas e interactuar con el Escalado automático en su nombre.

Uso de la política

Puede asociar AWSCodeDeployRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de mayo de 2015 a las 18:05 UTC
- Hora de edición: 16 de agosto de 2023 a las 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling>DeleteLifecycleHook",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:PutLifecycleHook",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:SuspendProcesses",
        "autoscaling:ResumeProcesses",
        "autoscaling:AttachLoadBalancers",
        "autoscaling:AttachLoadBalancerTargetGroups",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutWarmPool",
        "autoscaling:DescribeScalingActivities",
        "autoscaling>DeleteAutoScalingGroup",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:TerminateInstances",
        "tag:GetResources",
        "sns:Publish",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
```



```
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:DeregisterTargets"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployRoleForCloudFormation

AWSCodeDeployRoleForCloudFormation es una [política administrada por AWS](#) que: proporciona acceso al servicio CodeDeploy para invocar la función de Lambda en su nombre y realizar una implementación azul/verde a través de CloudFormation.

Uso de la política

Puede asociar AWSCodeDeployRoleForCloudFormation a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de mayo de 2020 a las 17:12 UTC

- Hora de edición: 19 de mayo de 2020 a las 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployRoleForECS

AWSCodeDeployRoleForECS es una [política administrada por AWS](#) que: concede acceso a todo el servicio CodeDeploy para realizar una implementación azul/verde de ECS en su nombre. Otorga acceso total a los servicios de soporte, como el acceso total para leer todos los objetos de S3, invocar todas las funciones de Lambda, publicar en todos los temas de SNS de la cuenta y actualizar todos los servicios de ECS.

Uso de la política

Puede asociar AWSCodeDeployRoleForECS a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2018 a las 20:40 UTC
- Hora de edición: 23 de septiembre de 2019 a las 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
```

```

    "ecs:DeleteTaskSet",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:ModifyListener",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:ModifyRule",
    "lambda:InvokeFunction",
    "cloudwatch:DescribeAlarms",
    "sns:Publish",
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource" : "*",
  "Effect" : "Allow"
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ecs-tasks.amazonaws.com"
      ]
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployRoleForECSLimited

AWSCodeDeployRoleForECSLimited es una [política administrada por AWS](#) que: proporciona acceso limitado al servicio CodeDeploy para realizar una implementación azul/verde de ECS en su nombre.

Uso de la política

Puede asociar AWSCodeDeployRoleForECSLimited a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2018 a las 20:42 UTC
- Hora de edición: 23 de septiembre de 2019 a las 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs>DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

```
  },
  {
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeListeners",
      "elasticloadbalancing:ModifyListener",
      "elasticloadbalancing:DescribeRules",
      "elasticloadbalancing:ModifyRule"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
      }
    },
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
```

```
"Resource" : [
  "arn:aws:iam::*:role/ecsTaskExecutionRole",
  "arn:aws:iam::*:role/ECSTaskExecution*"
],
"Condition" : {
  "StringLike" : {
    "iam:PassedToService" : [
      "ecs-tasks.amazonaws.com"
    ]
  }
}
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployRoleForLambda

AWSCodeDeployRoleForLambda es una [política administrada por AWS](#) que: otorga acceso al servicio CodeDeploy para realizar una implementación de Lambda en su nombre.

Uso de la política

Puede asociar AWSCodeDeployRoleForLambda a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de noviembre de 2017 a las 14:05 UTC
- Hora de edición: 3 de diciembre de 2019 a las 19:53 UTC

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

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig",
        "sns:Publish"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```



```
        "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
    }
  },
  "Effect" : "Allow"
},
{
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
  "Effect" : "Allow"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeDeployRoleForLambdaLimited

AWSCodeDeployRoleForLambdaLimited es una [política administrada por AWS](#) que: proporciona acceso limitado al servicio CodeDeploy para realizar una implementación de Lambda en su nombre.

Uso de la política

Puede asociar AWSCodeDeployRoleForLambdaLimited a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de agosto de 2020 a las 17:14 UTC
- Hora de edición: 17 de agosto de 2020 a las 17:14 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
    }
  },
  "Effect" : "Allow"
},
{
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
  "Effect" : "Allow"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodePipeline_FullAccess

AWSCodePipeline_FullAccesses una [política AWS gestionada](#) que: proporciona acceso total a AWS CodePipeline través de AWS Management Console.

Uso de la política

Puede asociar AWSCodePipeline_FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de agosto de 2020 a las 22:38 UTC
- Hora editada: 14 de marzo de 2024 a las 17:06 UTC

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

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListChangeSets",
        "cloudtrail:DescribeTrails",
        "codebuild:BatchGetProjects",
        "codebuild:CreateProject",
        "codebuild:ListCuratedEnvironmentImages",
        "codebuild:ListProjects",
        "codecommit:ListBranches",
        "codecommit:GetReferences",
        "codecommit:ListRepositories",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:ListClusters",
        "ecs:ListServices",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "iam:ListRoles",
        "iam:GetRole",
      ]
    }
  ]
}
```

```

        "lambda:ListFunctions",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:DescribeRule",
        "opsworks:DescribeApps",
        "opsworks:DescribeLayers",
        "opsworks:DescribeStacks",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsForResource",
        "codestar-notifications:ListEventTypes",
        "states:ListStateMachines"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Sid" : "CodePipelineAuthoringAccess"
},
{
    "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetObjectVersion",
        "s3:CreateBucket",
        "s3:PutBucketPolicy"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:s3::*:codepipeline-*",
    "Sid" : "CodePipelineArtifactsReadWriteAccess"
},
{
    "Action" : [
        "cloudtrail:PutEventSelectors",
        "cloudtrail:CreateTrail",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:StartLogging"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:cloudtrail::*:trail/codepipeline-source-trail",
    "Sid" : "CodePipelineSourceTrailReadWriteAccess"
},

```

```
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/service-role/cwe-role-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "events.amazonaws.com"
      ]
    }
  },
  "Sid" : "EventsIAMPassRole"
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "codepipeline.amazonaws.com"
      ]
    }
  },
  "Sid" : "CodePipelineIAMPassRole"
},
{
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events>DeleteRule",
    "events:DisableRule",
    "events:RemoveTargets"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:events::*:rule/codepipeline-*"
  ],
}
```

```

    "Sid" : "CodePipelineEventsReadWriteAccess"
  },
  {
    "Sid" : "CodeStarNotificationsReadWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:CreateNotificationRule",
      "codestar-notifications:DescribeNotificationRule",
      "codestar-notifications:UpdateNotificationRule",
      "codestar-notifications>DeleteNotificationRule",
      "codestar-notifications:Subscribe",
      "codestar-notifications:Unsubscribe"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
      }
    }
  },
  {
    "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:SetTopicAttributes"
    ],
    "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
  },
  {
    "Sid" : "CodeStarNotificationsChatbotAccess",
    "Effect" : "Allow",
    "Action" : [
      "chatbot:DescribeSlackChannelConfigurations",
      "chatbot:ListMicrosoftTeamsChannelConfigurations"
    ],
    "Resource" : "*"
  }
],
"Version" : "2012-10-17"
}

```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSCodePipeline_ReadOnlyAccess

AWSCodePipeline_ReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a AWS CodePipeline a través de la AWS Management Console.

Uso de la política

Puede asociar AWSCodePipeline_ReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de agosto de 2020 a las 22:25 UTC
- Hora de edición: 3 de agosto de 2020 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{  
  "Statement" : [  
    {  
      "Action": "codepipeline:ViewJobExecution",  
      "Resource": "arn:aws:codepipeline:*:*:*:job/*",  
      "Effect": "Allow"  
    }  
  ]  
}
```



```

{
  "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"
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodePipelineApproverAccess

AWSCodePipelineApproverAccess es una [política administrada por AWS](#) que: brinda acceso para ver y aprobar los cambios manuales en todos los pipelines

Uso de la política

Puede asociar AWSCodePipelineApproverAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de julio de 2016 a las 18:59 UTC
- Hora de edición: 2 de agosto de 2017 a las 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Action" : [
      "codepipeline:GetPipeline",
      "codepipeline:GetPipelineState",
      "codepipeline:GetPipelineExecution",
      "codepipeline:ListPipelineExecutions",
      "codepipeline:ListPipelines",
      "codepipeline:PutApprovalResult"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodePipelineCustomActionAccess

AWSCodePipelineCustomActionAccess es una [política administrada por AWS](#) que: proporciona acceso a acciones personalizadas para sondear la información de los trabajos (incluidas las credenciales temporales) e informar de las actualizaciones de estado a AWS CodePipeline.

Uso de la política

Puede asociar AWSCodePipelineCustomActionAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de julio de 2015 a las 17:02 UTC

- Hora de edición: 9 de julio de 2015 a las 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeStarFullAccess

AWSCodeStarFullAccess es una [política administrada por AWS](#) que: concede acceso total a AWS CodeStar a través de la AWS Management Console.

Uso de la política

Puede asociar AWSCodeStarFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de abril de 2017 a las 16:23 UTC
- Hora de edición: 28 de marzo de 2023 a las 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*"
      ]
    }
  ]
}
```

```
    "cloud9:ValidateEnvironmentName"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CodeStarCF",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStack*",
    "cloudformation:ListStacks*",
    "cloudformation:GetTemplateSummary"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awscodestar-*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeStarNotificationsServiceRolePolicy

AWSCodeStarNotificationsServiceRolePolicy es una [política administrada por AWS](#) que: permite que las notificaciones de AWS CodeStar accedan a los Eventos de Amazon CloudWatch en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de noviembre de 2019 a las 16:10 UTC
- Hora de edición: 19 de marzo de 2020 a las 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/awscodestarnotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeStarNotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
```

```

    "codecommit:GetCommentsForPullRequest",
    "codecommit:GetCommentsForComparedCommit",
    "chatbot:DescribeSlackChannelConfigurations",
    "chatbot:UpdateSlackChannelConfiguration",
    "codecommit:GetDifferences",
    "codepipeline:ListActionExecutions"
  ],
  "Resource" : "*",
  "Effect" : "Allow"
},
{
  "Action" : [
    "codecommit:GetFile"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotEquals" : {
      "aws:ResourceTag/ExcludeFileContentFromNotifications" : "true"
    }
  },
  "Effect" : "Allow"
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCodeStarServiceRole

AWSCodeStarServiceRole es una [política administrada por AWS](#): NO UTILIZAR. Política de rol de servicio de AWS CodeStar que otorga privilegios administrativos para que CodeStar gestione la IAM y otros recursos de servicio en nombre del cliente.

Uso de la política

Puede asociar AWSCodeStarServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de abril de 2017 a las 15:20 UTC
- Hora de edición: 20 de septiembre de 2021 a las 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProjectEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events>DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",

```

```

    "cloudformation:ExecuteChangeSet",
    "cloudformation>DeleteChangeSet",
    "cloudformation:GetTemplate"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awscodestar-*",
    "arn:aws:cloudformation:*:*:stack/awseb-*",
    "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
    "arn:aws:cloudformation:*:aws:transform/CodeStar*"
  ]
},
{
  "Sid" : "ProjectStackTemplate",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:GetTemplateSummary",
    "cloudformation:DescribeChangeSet"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ProjectQuickstarts",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::awscodestar-*/*"
  ]
},
{
  "Sid" : "ProjectS3Buckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:*"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-codestar-*",
    "arn:aws:s3:::elasticbeanstalk-*"
  ]
},
{
  "Sid" : "ProjectServices",
  "Effect" : "Allow",

```

```

    "Action" : [
      "codestar:*",
      "codecommit:*",
      "codepipeline:*",
      "codedeploy:*",
      "codebuild:*",
      "autoscaling:*",
      "cloudwatch:Put*",
      "ec2:*",
      "elasticbeanstalk:*",
      "elasticloadbalancing:*",
      "iam:ListRoles",
      "logs:*",
      "sns:*",
      "cloud9:CreateEnvironmentEC2",
      "cloud9>DeleteEnvironment",
      "cloud9:DescribeEnvironment*",
      "cloud9:ListEnvironments"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ProjectWorkerRoles",
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:GetRole",
      "iam:PassRole",
      "iam:GetRolePolicy",
      "iam:PutRolePolicy",
      "iam:SetDefaultPolicyVersion",
      "iam:CreatePolicy",
      "iam>DeletePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam>CreateInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/CodeStarWorker*",

```

```

    "arn:aws:iam::*:policy/CodeStarWorker*",
    "arn:aws:iam::*:instance-profile/awscodestar-*"
  ]
},
{
  "Sid" : "ProjectTeamMembers",
  "Effect" : "Allow",
  "Action" : [
    "iam:AttachUserPolicy",
    "iam:DetachUserPolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnEquals" : {
      "iam:PolicyArn" : [
        "arn:aws:iam::*:policy/CodeStar_*"
      ]
    }
  }
},
{
  "Sid" : "ProjectRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreatePolicy",
    "iam>DeletePolicy",
    "iam:CreatePolicyVersion",
    "iam>DeletePolicyVersion",
    "iam>ListEntitiesForPolicy",
    "iam>ListPolicyVersions",
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
  ],
  "Resource" : [
    "arn:aws:iam::*:policy/CodeStar_*"
  ]
},
{
  "Sid" : "InspectServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam>ListAttachedRolePolicies"
  ],
  "Resource" : [

```

```
    "arn:aws:iam::*:role/aws-codestar-service-role",
    "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
  ]
},
{
  "Sid" : "IAMLinkRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "cloud9.amazonaws.com"
    }
  }
},
{
  "Sid" : "DescribeConfigRuleForARN",
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConfigRules"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ProjectCodeStarConnections",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection",
    "codestar-connections:GetConnection"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ProjectCodeStarConnectionsPassConnections",
  "Effect" : "Allow",
  "Action" : "codestar-connections:PassConnection",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
    }
  }
}
```

```
    }  
  }  
} ]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCompromisedKeyQuarantine

AWSCompromisedKeyQuarantine es una [política administrada por AWS](#) que: deniega el acceso a determinadas acciones, que el equipo de AWS aplica en caso de que las credenciales de un usuario de IAM se vean comprometidas o estén expuestas públicamente. NO elimine esta política. En su lugar, siga las instrucciones especificadas en el correo electrónico que se le envió sobre este evento.

Uso de la política

Puede asociar AWSCompromisedKeyQuarantine a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de agosto de 2020 a las 18:04 UTC
- Hora de edición: 11 de agosto de 2020 a las 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateUser",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "lambda:CreateFunction",
        "lightsail:Create*",
        "lightsail:Start*",
        "lightsail>Delete*",
        "lightsail:Update*",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:DownloadDefaultKeyPair"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCompromisedKeyQuarantineV2

AWSCompromisedKeyQuarantineV2 es una [política administrada por AWS](#) que: deniega el acceso a determinadas acciones, que el equipo de AWS aplica en caso de que las credenciales de un usuario de IAM se vean comprometidas o estén expuestas públicamente. NO elimine esta política. En su lugar, siga las instrucciones especificadas en el caso de soporte que se le creó sobre este evento.

Uso de la política

Puede asociar AWSCompromisedKeyQuarantineV2 a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de abril de 2021 a las 22:30 UTC
- Hora de edición: 16 de marzo de 2023 a las 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
```

```

    "lambda:ListTags",
    "lambda:PutProvisionedConcurrencyConfig",
    "lambda:TagResource",
    "lambda:UntagResource",
    "lambda:UpdateFunctionCode",
    "lightsail:Create*",
    "lightsail:Delete*",
    "lightsail:DownloadDefaultKeyPair",
    "lightsail:GetInstanceAccessDetails",
    "lightsail:Start*",
    "lightsail:Update*",
    "organizations:CreateAccount",
    "organizations:CreateOrganization",
    "organizations:InviteAccountToOrganization",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketAcl",
    "s3:PutBucketOwnershipControls",
    "s3:DeleteBucketPolicy",
    "s3:ObjectOwnerOverrideToBucketOwner",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutBucketPolicy",
    "s3:ListAllMyBuckets",
    "ec2:PurchaseReservedInstancesOffering",
    "ec2:AcceptReservedInstancesExchangeQuote",
    "ec2:CreateReservedInstancesListing",
    "savingsplans:CreateSavingsPlan"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSConfigMultiAccountSetupPolicy

AWSConfigMultiAccountSetupPolicy es una [política administrada por AWS](#) que: permite que Config llame a los servicios de AWS e implemente recursos de configuración en toda la organización

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de junio de 2019 a las 18:03 UTC
- Hora de edición: 24 de febrero de 2023 a las 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "config:PutConfigRule",
    "config>DeleteConfigRule"
  ],
  "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
multiaccountsetup.amazonaws.com/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConfigurationRecorders"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListAccounts",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeAccount"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:PutConformancePack",
    "config>DeleteConformancePack"
  ],
  "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConformancePackStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
}
```

```

    "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "config-conforms.amazonaws.com"
      }
    }
  },
  {
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Effect" : "Allow",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ssm.amazonaws.com"
      }
    }
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSConfigRemediationServiceRolePolicy

AWSConfigRemediationServiceRolePolicy es una [política administrada AWS](#) que: permite que AWS Config corrija los recursos en incumplimiento en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de junio de 2019 a las 21:21 UTC
- Hora de edición: 18 de junio de 2019 a las 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  },
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Effect" : "Allow"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSConfigRoleForOrganizations

AWSConfigRoleForOrganizations es una [política administrada por AWS](#) que: permite que AWS Config llame a las API de AWS Organizations de solo lectura

Uso de la política

Puede asociar AWSConfigRoleForOrganizations a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de marzo de 2018 a las 22:53 UTC
- Hora de edición: 24 de noviembre de 2020 a las 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSConfigRulesExecutionRole

AWSConfigRulesExecutionRole es una [política administrada por AWS](#) que: permite que una función de Lambda de AWS acceda a la API de AWS Config y a las capturas de configuración que AWS Config entrega periódicamente a Amazon S3. Los roles que evalúan los cambios de configuración de las reglas personalizadas de Config requieren este acceso.

Uso de la política

Puede asociar AWSConfigRulesExecutionRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de marzo de 2016 a las 17:59 UTC
- Hora de edición: 13 de mayo de 2019 a las 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Put*",
        "config:Get*",
        "config:List*",
        "config:Describe*",
        "config:BatchGet*",
        "config:Select*"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSConfigServiceRolePolicy

AWSConfigServiceRolePolicy es una [política AWS gestionada](#) que: permite a Config llamar a AWS los servicios y recopilar configuraciones de recursos en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de mayo de 2018 a las 23:31 UTC
- Hora editada: 22 de febrero de 2024 a las 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Versión de la política

Versión de la política: v50 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
```

```
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"appconfig:ListExtensionAssociations",
"appconfig:ListHostedConfigurationVersions",
"appconfig:ListTagsForResource",
"appflow:DescribeConnectorProfiles",
"appflow:DescribeFlow",
"appflow:ListFlows",
"appflow:ListTagsForResource",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingPolicies",
"appmesh:DescribeGatewayRoute",
"appmesh:DescribeMesh",
"appmesh:DescribeRoute",
"appmesh:DescribeVirtualGateway",
"appmesh:DescribeVirtualNode",
"appmesh:DescribeVirtualRouter",
"appmesh:DescribeVirtualService",
"appmesh:ListGatewayRoutes",
"appmesh:ListMeshes",
"appmesh:ListRoutes",
"appmesh:ListTagsForResource",
"appmesh:ListVirtualGateways",
"appmesh:ListVirtualNodes",
"appmesh:ListVirtualRouters",
"appmesh:ListVirtualServices",
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"appstream:DescribeApplications",
"appstream:DescribeDirectoryConfigs",
"appstream:DescribeFleets",
"appstream:DescribeStacks",
"appstream:ListTagsForResource",
"appsync:GetApiCache",
"appsync:GetGraphQLApi",
"appsync:ListGraphQLApis",
"aps:DescribeAlertManagerDefinition",
"aps:DescribeLoggingConfiguration",
```

```
"APS:DescribeRuleGroupsNamespace",
"APS:DescribeWorkspace",
"aps:ListRuleGroupsNamespaces",
"aps:ListTagsForResource",
"APS:ListWorkspaces",
"athena:GetDataCatalog",
"athena:GetPreparedStatement",
"athena:GetWorkGroup",
"athena:ListDataCatalogs",
"athena:ListPreparedStatements",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"auditmanager:GetAccountStatus",
"auditmanager:GetAssessment",
"auditmanager:ListAssessments",
"autoscaling-plans:DescribeScalingPlanResources",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling-plans:GetScalingPlanResourceForecastData",
"autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeLaunchConfigurations",
"autoscaling:DescribeLifecycleHooks",
"autoscaling:DescribePolicies",
"autoscaling:DescribeScheduledActions",
"autoscaling:DescribeTags",
"autoscaling:DescribeWarmPool",
"backup-gateway:ListTagsForResource",
"backup-gateway:ListVirtualMachines",
"backup:DescribeBackupVault",
"backup:DescribeFramework",
"backup:DescribeProtectedResource",
"backup:DescribeRecoveryPoint",
"backup:DescribeReportPlan",
"backup:GetBackupPlan",
"backup:GetBackupSelection",
"backup:GetBackupVaultAccessPolicy",
"backup:GetBackupVaultNotifications",
"backup:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListFrameworks",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListReportPlans",
"backup:ListTags",
"batch:DescribeComputeEnvironments",
```

```
"batch:DescribeJobQueues",
"batch:DescribeSchedulingPolicies",
"batch:ListSchedulingPolicies",
"batch:ListTagsForResource",
"billingconductor:ListAccountAssociations",
"billingconductor:ListBillingGroups",
"billingconductor:ListCustomLineItems",
"billingconductor:ListPricingPlans",
"billingconductor:ListPricingRules",
"billingconductor:ListPricingRulesAssociatedToPricingPlan",
"billingconductor:ListTagsForResource",
"budgets:DescribeBudgetAction",
"budgets:DescribeBudgetActionsForAccount",
"budgets:DescribeBudgetActionsForBudget",
"budgets:ViewBudget",
"cassandra:Select",
"ce:GetAnomalyMonitors",
"ce:GetAnomalySubscriptions",
"cloud9:DescribeEnvironmentMemberships",
"cloud9:DescribeEnvironments",
"cloud9:ListEnvironments",
"cloud9:ListTagsForResource",
"cloudformation:DescribeType",
"cloudformation:GetResource",
"cloudformation:ListResources",
"cloudformation:ListStackResources",
"cloudformation:ListStacks",
"cloudformation:ListTypes",
"cloudfront:GetFunction",
"cloudfront:GetOriginAccessControl",
"cloudfront:GetResponseHeadersPolicy",
"cloudfront:ListDistributions",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListResponseHeadersPolicies",
"cloudfront:ListTagsForResource",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventDataStore",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListEventDataStores",
"cloudtrail:ListTags",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
```

```
"cloudwatch:DescribeAlarmsForMetric",
"cloudwatch:DescribeAnomalyDetectors",
"cloudwatch:GetDashboard",
"cloudwatch:GetMetricStream",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"cloudwatch:ListTagsForResource",
"codeartifact:DescribeRepository",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListDomains",
"codeartifact:ListPackages",
"codeartifact:ListPackageVersions",
"codeartifact:ListRepositories",
"codeartifact:ListTagsForResource",
"codebuild:BatchGetReportGroups",
"codebuild:ListReportGroups",
"codecommit:GetRepository",
"codecommit:GetRepositoryTriggers",
"codecommit:ListRepositories",
"codecommit:ListTagsForResource",
"codedeploy:GetDeploymentConfig",
"codeguru-profiler:DescribeProfilingGroup",
"codeguru-profiler:GetNotificationConfiguration",
"codeguru-profiler:GetPolicy",
"codeguru-profiler:ListProfilingGroups",
"codeguru-reviewer:DescribeRepositoryAssociation",
"codeguru-reviewer:ListRepositoryAssociations",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"cognito-identity:DescribeIdentityPool",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:GetPrincipalTagAttributeMap",
"cognito-identity:ListIdentityPools",
"cognito-identity:ListTagsForResource",
"cognito-idp:DescribeIdentityProvider",
"cognito-idp:DescribeResourceServer",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:DescribeUserPoolDomain",
"cognito-idp:GetGroup",
"cognito-idp:GetUserPoolMfaConfig",
"cognito-idp:ListGroups",
"cognito-idp:ListIdentityProviders",
```

```
"cognito-idp:ListResourceServers",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListUserPools",
"config:BatchGet*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:Put*",
"config:Select*",
"connect:DescribeEvaluationForm",
"connect:DescribeInstance",
"connect:DescribeInstanceStorageConfig",
"connect:DescribePhoneNumber",
"connect:DescribePrompt",
"connect:DescribeQuickConnect",
"connect:DescribeRule",
"connect:DescribeUser",
"connect:GetTaskTemplate",
"connect:ListApprovedOrigins",
"connect:ListEvaluationForms",
"connect:ListInstanceAttributes",
"connect:ListInstances",
"connect:ListInstanceStorageConfigs",
"connect:ListIntegrationAssociations",
"connect:ListPhoneNumbers",
"connect:ListPhoneNumbersV2",
"connect:ListPrompts",
"connect:ListQuickConnects",
"connect:ListRules",
"connect:ListSecurityKeys",
"connect:ListTagsForResource",
"connect:ListTaskTemplates",
"connect:ListUsers",
"connect:SearchAvailablePhoneNumbers",
"databrew:DescribeDataset",
"databrew:DescribeJob",
"databrew:DescribeProject",
"databrew:DescribeRecipe",
"databrew:DescribeRuleset",
"databrew:DescribeSchedule",
"databrew:ListDatasets",
"databrew:ListJobs",
"databrew:ListProjects",
```



```
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:ListRulesets",
"databrew:ListSchedules",
"datasync:DescribeAgent",
"datasync:DescribeLocationEfs",
"datasync:DescribeLocationFsxLustre",
"datasync:DescribeLocationFsxWindows",
"datasync:DescribeLocationHdfs",
"datasync:DescribeLocationNfs",
"datasync:DescribeLocationObjectStorage",
"datasync:DescribeLocationS3",
"datasync:DescribeLocationSmb",
"datasync:DescribeTask",
"datasync:ListAgents",
"datasync:ListLocations",
"datasync:ListTagsForResource",
"datasync:ListTasks",
"dax:DescribeClusters",
"dax:DescribeParameterGroups",
"dax:DescribeParameters",
"dax:DescribeSubnetGroups",
"dax:ListTags",
"detective:ListGraphs",
"detective:ListTagsForResource",
"devicefarm:GetInstanceProfile",
"devicefarm:GetNetworkProfile",
"devicefarm:GetProject",
"devicefarm:GetTestGridProject",
"devicefarm:ListInstanceProfiles",
"devicefarm:ListNetworkProfiles",
"devicefarm:ListProjects",
"devicefarm:ListTagsForResource",
"devicefarm:ListTestGridProjects",
"devops-guru:GetResourceCollection",
"dms:DescribeCertificates",
"dms:DescribeEndpoints",
"dms:DescribeEventSubscriptions",
"dms:DescribeReplicationInstances",
"dms:DescribeReplicationSubnetGroups",
"dms:DescribeReplicationTaskAssessmentRuns",
"dms:DescribeReplicationTasks",
"dms:ListTagsForResource",
"ds:DescribeDirectories",
```

```
"ds:DescribeDomainControllers",
"ds:DescribeEventTopics",
"ds:ListLogSubscriptions",
"ds:ListTagsForResource",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeGlobalTableSettings",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:DescribeTableReplicaAutoScaling",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:DescribeClientVpnAuthorizationRules",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeDhcpOptions",
"ec2:DescribeFleets",
"ec2:DescribeNetworkAcls",
"ec2:DescribePlacementGroups",
"ec2:DescribeRouteTables",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeTags",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeVolumeAttribute",
"ec2:DescribeVolumes",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetInstanceTypesFromInstanceRequirements",
"ec2:GetIpamPoolAllocations",
"ec2:GetIpamPoolCidrs",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ecr-public:DescribeRepositories",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribePullThroughCacheRules",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
```

```
"ecr:GetRegistryPolicy",
"ecr:GetRepositoryPolicy",
"ecr:ListTagsForResource",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:DescribeTaskSets",
"ecs:ListClusters",
"ecs:ListServices",
"ecs:ListTagsForResource",
"ecs:ListTaskDefinitionFamilies",
"ecs:ListTaskDefinitions",
"eks:DescribeAddon",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeIdentityProviderConfig",
"eks:DescribeNodegroup",
"eks:ListAddons",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListIdentityProviderConfigs",
"eks:ListNodegroups",
"eks:ListTagsForResource",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheParameters",
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticache:ListTagsForResource",
"elasticbeanstalk:DescribeConfigurationSettings",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
```

```
"elasticloadbalancing:DescribeListenerCertificates",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:DescribeSecurityConfiguration",
"elasticmapreduce:DescribeStep",
"elasticmapreduce:DescribeStudio",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:GetManagedScalingPolicy",
"elasticmapreduce:GetStudioSessionMapping",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstanceFleets",
"elasticmapreduce:ListInstanceGroups",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elasticmapreduce:ListSteps",
"elasticmapreduce:ListStudios",
"elasticmapreduce:ListStudioSessionMappings",
"emr-containers:DescribeVirtualCluster",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
"emr-serverless:ListApplications",
"es:DescribeDomain",
"es:DescribeDomains",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:GetCompatibleElasticsearchVersions",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListTags",
"events:DescribeApiDestination",
"events:DescribeArchive",
"events:DescribeConnection",
"events:DescribeEndpoint",
"events:DescribeEventBus",
"events:DescribeRule",
"events:ListApiDestinations",
```

```
"events:ListArchives",
"events:ListConnections",
"events:ListEndpoints",
"events:ListEventBuses",
"events:ListRules",
"events:ListTagsForResource",
"events:ListTargetsByRule",
"evidently:GetLaunch",
"evidently:GetProject",
"evidently:GetSegment",
"evidently:ListLaunches",
"evidently:ListProjects",
"evidently:ListSegments",
"evidently:ListTagsForResource",
"finSPACE:GetEnvironment",
"finSPACE:ListEnvironments",
"firehose:DescribeDeliveryStream",
"firehose:ListDeliveryStreams",
"firehose:ListTagsForDeliveryStream",
"fis:GetExperimentTemplate",
"fis:ListExperimentTemplates",
"fms:GetNotificationChannel",
"fms:GetPolicy",
"fms:ListPolicies",
"fms:ListTagsForResource",
"forecast:DescribeDataset",
"forecast:DescribeDatasetGroup",
"forecast:ListDatasetGroups",
"forecast:ListDatasets",
"forecast:ListTagsForResource",
"frauddetector:GetDetectors",
"frauddetector:GetDetectorVersion",
"frauddetector:GetEntityTypes",
"frauddetector:GetEventTypes",
"frauddetector:GetExternalModels",
"frauddetector:GetLabels",
"frauddetector:GetModels",
"frauddetector:GetOutcomes",
"frauddetector:GetRules",
"frauddetector:GetVariables",
"frauddetector:ListTagsForResource",
"fsx:DescribeBackups",
"fsx:DescribeDataRepositoryAssociations",
"fsx:DescribeFileSystems",
```

```
"fsx:DescribeSnapshots",
"fsx:DescribeStorageVirtualMachines",
"fsx:DescribeVolumes",
"fsx:ListTagsForResource",
"gamelift:DescribeAlias",
"gamelift:DescribeBuild",
"gamelift:DescribeFleetAttributes",
"gamelift:DescribeFleetCapacity",
"gamelift:DescribeFleetLocationAttributes",
"gamelift:DescribeFleetLocationCapacity",
"gamelift:DescribeFleetPortSettings",
"gamelift:DescribeGameServerGroup",
"gamelift:DescribeGameSessionQueues",
"gamelift:DescribeMatchmakingConfigurations",
"gamelift:DescribeMatchmakingRuleSets",
"gamelift:DescribeRuntimeConfiguration",
"gamelift:DescribeScript",
"gamelift:DescribeVpcPeeringAuthorizations",
"gamelift:DescribeVpcPeeringConnections",
"gamelift:ListAliases",
"gamelift:ListBuilds",
"gamelift:ListFleets",
"gamelift:ListGameServerGroups",
"gamelift:ListScripts",
"gamelift:ListTagsForResource",
"geo:DescribeGeofenceCollection",
"geo:DescribeMap",
"geo:DescribePlaceIndex",
"geo:DescribeRouteCalculator",
"geo:DescribeTracker",
"geo:ListGeofenceCollections",
"geo:ListMaps",
"geo:ListPlaceIndexes",
"geo:ListRouteCalculators",
"geo:ListTrackerConsumers",
"geo:ListTrackers",
"globalaccelerator:DescribeAccelerator",
"globalaccelerator:DescribeEndpointGroup",
"globalaccelerator:DescribeListener",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"globalaccelerator:ListTagsForResource",
"glue:BatchGetDevEndpoints",
```

```
"glue:BatchGetJobs",
"glue:BatchGetWorkflows",
"glue:GetClassifier",
"glue:GetClassifiers",
"glue:GetCrawler",
"glue:GetCrawlers",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetDevEndpoint",
"glue:GetDevEndpoints",
"glue:GetJob",
"glue:GetJobs",
"glue:GetMLTransform",
"glue:GetMLTransforms",
"glue:GetPartition",
"glue:GetPartitions",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTags",
"glue:GetWorkflow",
"glue:ListCrawlers",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
"glue:ListWorkflows",
"grafana:DescribeWorkspace",
"grafana:DescribeWorkspaceAuthentication",
"grafana:DescribeWorkspaceConfiguration",
"grafana:ListWorkspaces",
"greengrass:DescribeComponent",
"greengrass:GetComponent",
"greengrass:ListComponents",
"greengrass:ListComponentVersions",
"groundstation:GetConfig",
"groundstation:GetDataflowEndpointGroup",
"groundstation:GetMissionProfile",
"groundstation:ListConfigs",
"groundstation:ListDataflowEndpointGroups",
"groundstation:ListMissionProfiles",
"groundstation:ListTagsForResource",
"guardduty:DescribePublishingDestination",
"guardduty:GetAdministratorAccount",
"guardduty:GetDetector",
```

```
"guardduty:GetFilter",
"guardduty:GetFindings",
"guardduty:GetIPSet",
"guardduty:GetMasterAccount",
"guardduty:GetMemberDetectors",
"guardduty:GetMembers",
"guardduty:GetThreatIntelSet",
"guardduty:ListDetectors",
"guardduty:ListFilters",
"guardduty:ListFindings",
"guardduty:ListIPSets",
"guardduty:ListMembers",
"guardduty:ListOrganizationAdminAccounts",
"guardduty:ListPublishingDestinations",
"guardduty:ListTagsForResource",
"guardduty:ListThreatIntelSets",
"healthlake:DescribeFHIRDatastore",
"healthlake:ListFHIRDatastores",
"healthlake:ListTagsForResource",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetGroup",
"iam:GetGroupPolicy",
"iam:GetInstanceProfile",
"iam:GetOpenIDConnectProvider",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetSAMLProvider",
"iam:GetServerCertificate",
"iam:GetUser",
"iam:GetUserPolicy",
"iam:ListAccessKeys",
"iam:ListAttachedGroupPolicies",
"iam:ListAttachedRolePolicies",
"iam:ListAttachedUserPolicies",
"iam:ListEntitiesForPolicy",
"iam:ListGroupPolicies",
"iam:ListGroups",
"iam:ListGroupsForUser",
```



```
"iam:ListInstanceProfiles",
"iam:ListInstanceProfilesForRole",
"iam:ListInstanceProfileTags",
"iam:ListMFADevices",
"iam:ListMFADeviceTags",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicyVersions",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"imagebuilder:GetComponent",
"imagebuilder:GetContainerRecipe",
"imagebuilder:GetDistributionConfiguration",
"imagebuilder:GetImage",
"imagebuilder:GetImagePipeline",
"imagebuilder:GetImageRecipe",
"imagebuilder:GetInfrastructureConfiguration",
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponents",
"imagebuilder:ListContainerRecipes",
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"inspector2:BatchGetAccountStatus",
"inspector2:GetDelegatedAdminAccount",
"inspector2:ListFilters",
"inspector2:ListMembers",
"iot:DescribeAccountAuditConfiguration",
"iot:DescribeAuthorizer",
"iot:DescribeCACertificate",
"iot:DescribeCertificate",
"iot:DescribeCustomMetric",
"iot:DescribeDimension",
"iot:DescribeDomainConfiguration",
"iot:DescribeFleetMetric",
"iot:DescribeJobTemplate",
"iot:DescribeMitigationAction",
```

```
"iot:DescribeProvisioningTemplate",
"iot:DescribeRoleAlias",
"iot:DescribeScheduledAudit",
"iot:DescribeSecurityProfile",
"iot:GetPolicy",
"iot:GetTopicRule",
"iot:GetTopicRuleDestination",
"iot:ListAuthorizers",
"iot:ListCACertificates",
"iot:ListCertificates",
"iot:ListCustomMetrics",
"iot:ListDimensions",
"iot:ListDomainConfigurations",
"iot:ListFleetMetrics",
"iot:ListJobTemplates",
"iot:ListMitigationActions",
"iot:ListPolicies",
"iot:ListProvisioningTemplates",
"iot:ListRoleAliases",
"iot:ListScheduledAudits",
"iot:ListSecurityProfiles",
"iot:ListSecurityProfilesForTarget",
"iot:ListTagsForResource",
"iot:ListTargetsForSecurityProfile",
"iot:ListTopicRuleDestinations",
"iot:ListTopicRules",
"iot:ListV2LoggingLevels",
"iot:ValidateSecurityProfileBehaviors",
"iotanalytics:DescribeChannel",
"iotanalytics:DescribeDataset",
"iotanalytics:DescribeDatastore",
"iotanalytics:DescribePipeline",
"iotanalytics:ListChannels",
"iotanalytics:ListDatasets",
"iotanalytics:ListDatastores",
"iotanalytics:ListPipelines",
"iotanalytics:ListTagsForResource",
"iotevents:DescribeAlarmModel",
"iotevents:DescribeDetectorModel",
"iotevents:DescribeInput",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iotevents:ListTagsForResource",
```

```
"iotsitewise:DescribeAccessPolicy",
"iotsitewise:DescribeAsset",
"iotsitewise:DescribeAssetModel",
"iotsitewise:DescribeDashboard",
"iotsitewise:DescribeGateway",
"iotsitewise:DescribePortal",
"iotsitewise:DescribeProject",
"iotsitewise:ListAccessPolicies",
"iotsitewise:ListAssetModels",
"iotsitewise:ListAssets",
"iotsitewise:ListDashboards",
"iotsitewise:ListGateways",
"iotsitewise:ListPortals",
"iotsitewise:ListProjectAssets",
"iotsitewise:ListProjects",
"iotsitewise:ListTagsForResource",
"iottwinmaker:GetComponentType",
"iottwinmaker:GetEntity",
"iottwinmaker:GetScene",
"iottwinmaker:GetSyncJob",
"iottwinmaker:GetWorkspace",
"iottwinmaker:ListComponentTypes",
"iottwinmaker:ListEntities",
"iottwinmaker:ListScenes",
"iottwinmaker:ListSyncJobs",
"iottwinmaker:ListTagsForResource",
"iottwinmaker:ListWorkspaces",
"iotwireless:GetFuotaTask",
"iotwireless:GetMulticastGroup",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:GetChannel",
"ivs:GetPlaybackKeyPair",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamKey",
"ivs:ListChannels",
"ivs:ListPlaybackKeyPairs",
```

```
"ivs:ListRecordingConfigurations",
"ivs:ListStreamKeys",
"ivs:ListTagsForResource",
"kafka:DescribeCluster",
"kafka:DescribeClusterV2",
"kafka:DescribeConfiguration",
"kafka:DescribeConfigurationRevision",
"kafka:DescribeVpcConnection",
"kafka:GetClusterPolicy",
"kafka:ListClusters",
"kafka:ListClustersV2",
"kafka:ListConfigurations",
"kafka:ListScramSecrets",
"kafka:ListTagsForResource",
"kafka:ListVpcConnections",
"kafkaconnect:DescribeConnector",
"kafkaconnect:ListConnectors",
"kendra:DescribeIndex",
"kendra:ListIndices",
"kendra:ListTagsForResource",
"kinesis:DescribeStreamConsumer",
"kinesis:DescribeStreamSummary",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
"kinesisanalytics:DescribeApplication",
"kinesisanalytics:ListApplications",
"kinesisanalytics:ListTagsForResource",
"kinesisvideo:DescribeSignalingChannel",
"kinesisvideo:DescribeStream",
"kinesisvideo:ListSignalingChannels",
"kinesisvideo:ListStreams",
"kinesisvideo:ListTagsForResource",
"kinesisvideo:ListTagsForStream",
"kms:DescribeKey",
"kms:GetKeyPolicy",
"kms:GetKeyRotationStatus",
"kms:ListAliases",
"kms:ListKeys",
"kms:ListResourceTags",
"lakeformation:DescribeResource",
"lakeformation:GetDataLakeSettings",
"lakeformation:ListPermissions",
"lakeformation:ListResources",
```

```
"lambda:GetAlias",
"lambda:GetCodeSigningConfig",
"lambda:GetFunction",
"lambda:GetFunctionCodeSigningConfig",
"lambda:GetLayerVersion",
"lambda:GetPolicy",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"lambda:ListFunctions",
"lambda:ListLayers",
"lambda:ListLayerVersions",
"lambda:ListTags",
"lambda:ListVersionsByFunction",
"lex:DescribeBot",
"lex:DescribeBotAlias",
"lex:DescribeBotVersion",
"lex:DescribeResourcePolicy",
"lex:ListBotAliases",
"lex:ListBotLocales",
"lex:ListBots",
"lex:ListBotVersions",
"lex:ListTagsForResource",
"license-manager:GetGrant",
"license-manager:GetLicense",
"license-manager:ListDistributedGrants",
"license-manager:ListLicenses",
"license-manager:ListReceivedGrants",
"lightsail:GetAlarms",
"lightsail:GetBuckets",
"lightsail:GetCertificates",
"lightsail:GetContainerServices",
"lightsail:GetDisk",
"lightsail:GetDisks",
"lightsail:GetDistributions",
"lightsail:GetInstance",
"lightsail:GetInstances",
"lightsail:GetKeyPair",
"lightsail:GetLoadBalancer",
"lightsail:GetLoadBalancers",
"lightsail:GetLoadBalancerTlsCertificates",
"lightsail:GetRelationalDatabase",
"lightsail:GetRelationalDatabaseParameters",
"lightsail:GetRelationalDatabases",
"lightsail:GetStaticIp",
```

```
"lightsail:GetStaticIps",
"logs:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"logs:GetDataProtectionPolicy",
"logs:GetLogDelivery",
"logs:ListLogDeliveries",
"logs:ListTagsLogGroup",
"lookoutequipment:DescribeInferenceScheduler",
"lookoutequipment:ListTagsForResource",
"lookoutmetrics:DescribeAlert",
"lookoutmetrics:DescribeAnomalyDetector",
"lookoutmetrics:ListAlerts",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutmetrics:ListMetricSets",
"lookoutmetrics:ListTagsForResource",
"lookoutvision:DescribeProject",
"lookoutvision:ListProjects",
"m2:GetEnvironment",
"m2:ListEnvironments",
"m2:ListTagsForResource",
"macie2:DescribeOrganizationConfiguration",
"macie2:GetAutomatedDiscoveryConfiguration",
"macie2:GetClassificationExportConfiguration",
"macie2:GetCustomDataIdentifier",
"macie2:GetFindingsPublicationConfiguration",
"macie2:GetMacieSession",
"macie2:ListCustomDataIdentifiers",
"macie2:ListTagsForResource",
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
"managedblockchain:GetNode",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNodes",
"mediaconnect:DescribeFlow",
"mediaconnect:ListFlows",
"mediaconnect:ListTagsForResource",
"mediapackage-vod:DescribePackagingConfiguration",
"mediapackage-vod:DescribePackagingGroup",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mediapackage-vod:ListTagsForResource",
"mediatailor:GetPlaybackConfiguration",
```

```
"mediatailor:ListPlaybackConfigurations",
"memorydb:DescribeAcls",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeParameters",
"memorydb:DescribeSubnetGroups",
"memorydb:DescribeUsers",
"memorydb:ListTags",
"mobiletargeting:GetApp",
"mobiletargeting:GetApplicationSettings",
"mobiletargeting:GetApps",
"mobiletargeting:GetCampaign",
"mobiletargeting:GetCampaigns",
"mobiletargeting:GetEmailChannel",
"mobiletargeting:GetEmailTemplate",
"mobiletargeting:GetEventStream",
"mobiletargeting:GetInAppTemplate",
"mobiletargeting:GetSegment",
"mobiletargeting:GetSegments",
"mobiletargeting:ListTagsForResource",
"mobiletargeting:ListTemplates",
"mq:DescribeBroker",
"mq:ListBrokers",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:ListFirewalls",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetConnectPeer",
"networkmanager:GetCustomerGatewayAssociations",
"networkmanager:GetDevices",
"networkmanager:GetLinkAssociations",
"networkmanager:GetLinks",
"networkmanager:GetSites",
"networkmanager:GetTransitGatewayRegistrations",
"networkmanager:ListConnectPeers",
"networkmanager:ListTagsForResource",
"nimble:GetLaunchProfile",
"nimble:GetLaunchProfileDetails",
"nimble:GetStreamingImage",
"nimble:GetStudio",
"nimble:GetStudioComponent",
"nimble:ListLaunchProfiles",
"nimble:ListStreamingImages",
"nimble:ListStudioComponents",
"nimble:ListStudios",
```

```
"opsworks:DescribeInstances",
"opsworks:DescribeLayers",
"opsworks:DescribeTimeBasedAutoScaling",
"opsworks:DescribeVolumes",
"opsworks:ListTags",
"organizations:DescribeAccount",
"organizations:DescribeEffectivePolicy",
"organizations:DescribeOrganization",
"organizations:DescribeOrganizationalUnit",
"organizations:DescribePolicy",
"organizations:DescribeResourcePolicy",
"organizations:ListAccounts",
"organizations:ListAccountsForParent",
"organizations:ListDelegatedAdministrators",
"organizations:ListOrganizationalUnitsForParent",
"organizations:ListParents",
"organizations:ListPolicies",
"organizations:ListPoliciesForTarget",
"organizations:ListRoots",
"organizations:ListTagsForResource",
"organizations:ListTargetsForPolicy",
"panorama:DescribeApplicationInstance",
"panorama:DescribeApplicationInstanceDetails",
"panorama:DescribePackage",
"panorama:DescribePackageVersion",
"panorama:ListApplicationInstances",
"panorama:ListNodes",
"panorama:ListPackages",
"personalize:DescribeDataset",
"personalize:DescribeDatasetGroup",
"personalize:DescribeSchema",
"personalize:DescribeSolution",
"personalize:ListDatasetGroups",
"personalize:ListDatasetImportJobs",
"personalize:ListDatasets",
"personalize:ListSchemas",
"personalize:ListSolutions",
"personalize:ListTagsForResource",
"profile:GetDomain",
"profile:GetIntegration",
"profile:GetProfileObjectType",
"profile:ListDomains",
"profile:ListIntegrations",
"profile:ListProfileObjectTypes",
```



```
"profile:ListTagsForResource",
"quicksight:DescribeAccountSubscription",
"quicksight:DescribeAnalysis",
"quicksight:DescribeAnalysisPermissions",
"quicksight:DescribeDashboard",
"quicksight:DescribeDashboardPermissions",
"quicksight:DescribeDataSet",
"quicksight:DescribeDataSetPermissions",
"quicksight:DescribeDataSetRefreshProperties",
"quicksight:DescribeDataSource",
"quicksight:DescribeDataSourcePermissions",
"quicksight:DescribeTemplate",
"quicksight:DescribeTemplatePermissions",
"quicksight:DescribeTheme",
"quicksight:DescribeThemePermissions",
"quicksight:ListAnalyses",
"quicksight:ListDashboards",
"quicksight:ListDataSets",
"quicksight:ListDataSources",
"quicksight:ListTagsForResource",
"quicksight:ListTemplates",
"quicksight:ListThemes",
"ram:GetPermission",
"ram:GetResourceShareAssociations",
"ram:GetResourceShares",
"ram:ListPermissionAssociations",
"ram:ListPermissions",
"ram:ListPermissionVersions",
"ram:ListResources",
"ram:ListResourceSharePermissions",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyEndpoints",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshotAttributes",
"rds:DescribeDBSnapshots",
```

```
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:ListTagsForResource",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListWorkgroups",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusterParameters",
"redshift:DescribeClusters",
"redshift:DescribeClusterSecurityGroups",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEndpointAccess",
"redshift:DescribeEndpointAuthorization",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeLoggingStatus",
"redshift:DescribeScheduledActions",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListServices",
"rekognition:DescribeStreamProcessor",
"rekognition:ListStreamProcessors",
"rekognition:ListTagsForResource",
"resiliencehub:DescribeApp",
"resiliencehub:DescribeAppVersionTemplate",
"resiliencehub:DescribeResiliencyPolicy",
"resiliencehub:ListApps",
"resiliencehub:ListAppVersionResourceMappings",
"resiliencehub:ListResiliencyPolicies",
"resiliencehub:ListTagsForResource",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListTagsForResource",
"resource-groups:GetGroup",
"resource-groups:GetGroupConfiguration",
"resource-groups:GetGroupQuery",
"resource-groups:GetTags",
```

```
"resource-groups:ListGroupResources",
"resource-groups:ListGroups",
"robomaker:DescribeRobotApplication",
"robomaker:DescribeSimulationApplication",
"robomaker:ListRobotApplications",
"robomaker:ListSimulationApplications",
"route53-recovery-control-config:DescribeCluster",
"route53-recovery-control-config:DescribeControlPanel",
"route53-recovery-control-config:DescribeRoutingControl",
"route53-recovery-control-config:DescribeSafetyRule",
"route53-recovery-control-config:ListClusters",
"route53-recovery-control-config:ListControlPanels",
"route53-recovery-control-config:ListRoutingControls",
"route53-recovery-control-config:ListSafetyRules",
"route53-recovery-control-config:ListTagsForResource",
"route53-recovery-readiness:GetCell",
"route53-recovery-readiness:GetReadinessCheck",
"route53-recovery-readiness:GetRecoveryGroup",
"route53-recovery-readiness:GetResourceSet",
"route53-recovery-readiness:ListCells",
"route53-recovery-readiness:ListReadinessChecks",
"route53-recovery-readiness:ListRecoveryGroups",
"route53-recovery-readiness:ListResourceSets",
"route53:GetChange",
"route53:GetDNSSEC",
"route53:GetHealthCheck",
"route53:GetHostedZone",
"route53:ListCidrBlocks",
"route53:ListCidrCollections",
"route53:ListCidrLocations",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53:ListHostedZonesByName",
"route53:ListQueryLoggingConfigs",
"route53:ListResourceRecordSets",
"route53:ListTagsForResource",
"route53resolver:GetFirewallDomainList",
"route53resolver:GetFirewallRuleGroup",
"route53resolver:GetFirewallRuleGroupAssociation",
"route53resolver:GetResolverDnssecConfig",
"route53resolver:GetResolverEndpoint",
"route53resolver:GetResolverQueryLogConfig",
"route53resolver:GetResolverQueryLogConfigAssociation",
"route53resolver:GetResolverRule",
```

```
"route53resolver:GetResolverRuleAssociation",
"route53resolver:ListFirewallDomainLists",
"route53resolver:ListFirewallDomains",
"route53resolver:ListFirewallRuleGroupAssociations",
"route53resolver:ListFirewallRuleGroups",
"route53resolver:ListFirewallRules",
"route53resolver:ListResolverDnssecConfigs",
"route53resolver:ListResolverEndpointIpAddresses",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverQueryLogConfigAssociations",
"route53resolver:ListResolverQueryLogConfigs",
"route53resolver:ListResolverRuleAssociations",
"route53resolver:ListResolverRules",
"route53resolver:ListTagsForResource",
"rum:GetAppMonitor",
"rum:GetAppMonitorData",
"rum:ListAppMonitors",
"rum:ListTagsForResource",
"s3-outposts:GetAccessPoint",
"s3-outposts:GetAccessPointPolicy",
"s3-outposts:GetBucket",
"s3-outposts:GetBucketPolicy",
"s3-outposts:GetBucketTagging",
"s3-outposts:GetLifecycleConfiguration",
"s3-outposts:ListAccessPoints",
"s3-outposts:ListEndpoints",
"s3-outposts:ListRegionalBuckets",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointForObjectLambda",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyForObjectLambda",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccessPointPolicyStatusForObjectLambda",
"s3:GetAccountPublicAccessBlock",
"s3:GetBucketAcl",
"s3:GetBucketCORS",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketNotification",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketPolicy",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
```

```
"s3:GetBucketRequestPayment",
"s3:GetBucketTagging",
"s3:GetBucketVersioning",
"s3:GetBucketWebsite",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMultiRegionAccessPoint",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetMultiRegionAccessPointPolicyStatus",
"s3:GetReplicationConfiguration",
"s3:GetStorageLensConfiguration",
"s3:GetStorageLensConfigurationTagging",
"s3:ListAccessPoints",
"s3:ListAccessPointsForObjectLambda",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListMultiRegionAccessPoints",
"s3:ListStorageLensConfigurations",
"s3express:GetBucketPolicy",
"s3express:ListAllMyDirectoryBuckets",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceExperiment",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribeProject",
"sagemaker:DescribeWorkteam",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListCodeRepositories",
"sagemaker:ListDataQualityJobDefinitions",
```

```
"sagemaker:ListDeviceFleets",
"sagemaker:ListDomains",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListFeatureGroups",
"sagemaker:ListImages",
"sagemaker:ListImageVersions",
"sagemaker:ListInferenceExperiments",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelines",
"sagemaker:ListProjects",
"sagemaker:ListTags",
"sagemaker:ListWorkteams",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemas",
"sdb:GetAttributes",
"sdb:ListDomains",
"secretsmanager:ListSecrets",
"secretsmanager:ListSecretVersionIds",
"securityhub:DescribeHub",
"servicecatalog:DescribePortfolioShares",
"servicediscovery:GetInstance",
"servicediscovery:GetNamespace",
"servicediscovery:GetService",
"servicediscovery:ListInstances",
"servicediscovery:ListNamespaces",
"servicediscovery:ListServices",
"servicediscovery:ListTagsForResource",
"ses:DescribeReceiptRule",
"ses:DescribeReceiptRuleSet",
"ses:GetConfigurationSet",
"ses:GetConfigurationSetEventDestinations",
"ses:GetContactList",
```

```
"ses:GetEmailTemplate",
"ses:GetTemplate",
"ses:ListConfigurationSets",
"ses:ListContactLists",
"ses:ListEmailTemplates",
"ses:ListReceiptFilters",
"ses:ListReceiptRuleSets",
"ses:ListTemplates",
"shield:DescribeDRTAccess",
"shield:DescribeProtection",
"shield:DescribeSubscription",
"signer:GetSigningProfile",
"signer:ListProfilePermissions",
"signer:ListSigningProfiles",
"sns:GetDataProtectionPolicy",
"sns:GetSMSSandboxAccountStatus",
"sns:GetSubscriptionAttributes",
"sns:GetTopicAttributes",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTagsForResource",
"sns:ListTopics",
"sqs:GetQueueAttributes",
"sqs:ListQueues",
"sqs:ListQueueTags",
"ssm:DescribeAutomationExecutions",
"ssm:DescribeDocument",
"ssm:DescribeDocumentPermission",
"ssm:DescribeParameters",
"ssm:GetAutomationExecution",
"ssm:GetDocument",
"ssm:ListDocuments",
"ssm:ListTagsForResource",
"sso:DescribeInstanceAccessControlAttributeConfiguration",
"sso:DescribePermissionSet",
"sso:GetInlinePolicyForPermissionSet",
"sso:ListManagedPoliciesInPermissionSet",
"sso:ListPermissionSets",
"sso:ListTagsForResource",
"states:DescribeActivity",
"states:DescribeStateMachine",
"states:ListActivities",
"states:ListStateMachines",
"states:ListTagsForResource",
```

```
"storagegateway:ListGateways",
"storagegateway:ListTagsForResource",
"storagegateway:ListVolumes",
"sts:GetCallerIdentity",
"support:DescribeCases",
"synthetics:DescribeCanaries",
"synthetics:DescribeCanariesLastRun",
"synthetics:DescribeRuntimeVersions",
"synthetics:GetCanary",
"synthetics:GetCanaryRuns",
"synthetics:GetGroup",
"synthetics:ListAssociatedGroups",
"synthetics:ListGroupResources",
"synthetics:ListGroups",
"synthetics:ListTagsForResource",
"tag:GetResources",
"timestream:DescribeDatabase",
"timestream:DescribeEndpoints",
"timestream:DescribeTable",
"timestream:ListDatabases",
"timestream:ListTables",
"timestream:ListTagsForResource",
"transfer:DescribeAgreement",
"transfer:DescribeCertificate",
"transfer:DescribeConnector",
"transfer:DescribeProfile",
"transfer:DescribeServer",
"transfer:DescribeUser",
"transfer:DescribeWorkflow",
"transfer:ListAgreements",
"transfer:ListCertificates",
"transfer:ListConnectors",
"transfer:ListProfiles",
"transfer:ListServers",
"transfer:ListTagsForResource",
"transfer:ListUsers",
"transfer:ListWorkflows",
"voiceid:DescribeDomain",
"voiceid:ListTagsForResource",
"waf-regional:GetLoggingConfiguration",
"waf-regional:GetWebACL",
"waf-regional:GetWebACLForResource",
"waf-regional:ListLoggingConfigurations",
"waf:GetLoggingConfiguration",
```



```

    "waf:GetWebACL",
    "wafv2:GetLoggingConfiguration",
    "wafv2:GetRuleGroup",
    "wafv2:ListRuleGroups",
    "wafv2:ListTagsForResource",
    "workspaces:DescribeConnectionAliases",
    "workspaces:DescribeTags",
    "workspaces:DescribeWorkspaces"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSConfigSLRLogStatementID",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:CreateLogGroup"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
},
{
  "Sid" : "AWSConfigSLRLogEventStatementID",
  "Effect" : "Allow",
  "Action" : "logs:PutLogEvents",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
},
{
  "Sid" : "AWSConfigSLRApiGatewayStatementID",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*:*/apis",
    "arn:aws:apigateway:*:*/apis/*",
    "arn:aws:apigateway:*:*/apis/*/integrations",
    "arn:aws:apigateway:*:*/apis/*/integrations/*",
    "arn:aws:apigateway:*:*/domainnames",
    "arn:aws:apigateway:*:*/clientcertificates",
    "arn:aws:apigateway:*:*/clientcertificates/*",
    "arn:aws:apigateway:*:*/restapis",
    "arn:aws:apigateway:*:*/restapis/*/resources/*/methods/*",
    "arn:aws:apigateway:*:*/restapis/*",

```

```

    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/resources",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
    "arn:aws:apigateway:*::/restapis/*/resources/*",
    "arn:aws:apigateway:*::/apis/*/routes/*",
    "arn:aws:apigateway:*::/apis/*/routes",
    "arn:aws:apigateway:*::/v2/apis/*/routes",
    "arn:aws:apigateway:*::/v2/apis/*/routes/*",
    "arn:aws:apigateway:*::/v2/apis",
    "arn:aws:apigateway:*::/v2/apis/*",
    "arn:aws:apigateway:*::/v2/apis/*/integrations",
    "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
  ]
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSConfigUserAccess

AWSConfigUserAccess es una [política administrada por AWS](#) que: proporciona al usuario acceso para utilizar AWS Config, incluida la búsqueda por etiquetas en los recursos y la lectura de todas las etiquetas. Esto no otorga permiso para configurar AWS Config, lo cual requiere de privilegios administrativos.

Uso de la política

Puede asociar AWSConfigUserAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de febrero de 2015 a las 19:38 UTC

- Hora de edición: 18 de marzo de 2019 a las 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSConnector

AWSConnectores una [política AWS gestionada](#) que: permite un amplio acceso de lectura y escritura a TODOS los objetos de EC2, el acceso de lectura y escritura a los buckets de S3 que comiencen por «import-to-ec2» y la posibilidad de enumerar todos los buckets de S3 para que el Connector importe las AWS máquinas virtuales en su nombre.

Uso de la política

Puede asociar AWSConnector a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de febrero de 2015 a las 17:14 UTC
- Hora de edición: 28 de septiembre de 2015 a las 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:DeleteBucket",
      "s3:DeleteObject",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:AbortMultipartUpload",
      "s3:ListBucketMultipartUploads",
      "s3:ListMultipartUploadParts"
    ],
    "Resource" : "arn:aws:s3:::import-to-ec2-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CancelConversionTask",
      "ec2:CancelExportTask",
      "ec2:CreateImage",
      "ec2:CreateInstanceExportTask",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2>DeleteTags",
      "ec2>DeleteVolume",
      "ec2:DescribeConversionTasks",
      "ec2:DescribeExportTasks",
      "ec2:DescribeImages",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstances",
      "ec2:DescribeRegions",
```

```

    "ec2:DescribeTags",
    "ec2:DetachVolume",
    "ec2:ImportInstance",
    "ec2:ImportVolume",
    "ec2:ModifyInstanceAttribute",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ImportImage",
    "ec2:DescribeImportImageTasks",
    "ec2:DeregisterImage",
    "ec2:DescribeSnapshots",
    "ec2>DeleteSnapshot",
    "ec2:CancelImportTask",
    "ec2:ImportSnapshot",
    "ec2:DescribeImportSnapshotTasks"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "SNS:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSControlTowerAccountServiceRolePolicy

AWSControlTowerAccountServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Control Tower llame en su nombre a los servicios de AWS que proporcionan una configuración de cuentas automatizada y un gobierno centralizado.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de junio de 2023 a las 22:04 UTC
- Hora de edición: 5 de junio de 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```

    "events:source" : "aws.securityhub"
  },
  "Null" : {
    "events:detail-type" : "false"
  },
  "StringEquals" : {
    "events:ManagedBy" : "controltower.amazonaws.com",
    "events:detail-type" : "Security Hub Findings - Imported"
  }
}
},
{
  "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "controltower.amazonaws.com"
    }
  }
}
},
{
  "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
}
},
{
  "Sid" : "AllowControlTowerToPublishSecurityNotifications",
  "Effect" : "Allow",
  "Action" : "sns:publish",
  "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
  "Condition" : {
    "StringEquals" : {

```



```
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
    }
}
},
{
    "Sid" : "AllowActionsForSecurityHubIntegration",
    "Effect" : "Allow",
    "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
    ],
    "Resource" : "arn:aws:securityhub:*:*:hub/default"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSControlTowerServiceRolePolicy

AWSControlTowerServiceRolePolicy es una [política administrada por AWS](#) que: concede acceso a los recursos de AWS gestionados o utilizados por AWS Control Tower

Uso de la política

Puede asociar AWSControlTowerServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 3 de mayo de 2019 a las 18:19 UTC
- Hora de edición: 12 de abril de 2023 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation>DeleteStack",
        "cloudformation>DeleteStackInstances",
        "cloudformation>DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation>DeleteStack",
        "cloudformation>DeleteStackInstances",
```

```

    "cloudformation:DeleteStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:GetTemplate",
    "cloudformation:ListStackInstances",
    "cloudformation:UpdateStack",
    "cloudformation:UpdateStackInstances",
    "cloudformation:UpdateStackSet"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/AWSControlTower*/**",
    "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/**",
    "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
    "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/**"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:CreateTrail",
    "cloudtrail>DeleteTrail",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:StartLogging",
    "cloudtrail:StopLogging",
    "cloudtrail:UpdateTrail",
    "cloudtrail:PutEventSelectors",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
    "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-controltower*/**"
  ]
}

```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sts:AssumeRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSControlTowerExecution",
    "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:DescribeTrails",
    "ec2:DescribeAvailabilityZones",
    "iam:ListRoles",
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups",
    "organizations:CreateAccount",
    "organizations:DescribeAccount",
    "organizations:DescribeCreateAccountStatus",
    "organizations:DescribeOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribePolicy",
    "organizations:ListAccounts",
    "organizations:ListAccountsForParent",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListChildren",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListParents",
    "organizations:ListPoliciesForTarget",
    "organizations:ListTargetsForPolicy",
    "organizations:ListRoots",
    "organizations:MoveAccount",
    "servicecatalog:AssociatePrincipalWithPortfolio"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
```

```

    "iam:GetUser",
    "iam:ListAttachedRolePolicies",
    "iam:GetRolePolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
    "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
    "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:DeleteConfigurationAggregator",
    "config:PutConfigurationAggregator",
    "config:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "organizations:ServicePrincipal" : [
        "config.amazonaws.com",
        "cloudtrail.amazonaws.com"
      ]
    }
  }
}

```

```

    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "account:EnableRegion",
    "account:ListRegions",
    "account:GetRegionOptStatus"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSCostAndUsageReportAutomationPolicy

AWSCostAndUsageReportAutomationPolicy es una [política administrada AWS](#) que: otorga permisos para describir la organización de la cuenta, crear grupos de S3 para el programa MAP y

aplicarle etiquetas, crear un informe de costos y uso, y describir las definiciones de los informes de costo y uso.

Uso de la política

Puede asociar `AWSCostAndUsageReportAutomationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de noviembre de 2021 a las 21:27 UTC
- Hora de edición: 1 de noviembre de 2021 a las 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",

```

```

    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:ListBucket",
    "s3:CreateBucket"
  ],
  "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cur:PutReportDefinition",
    "cur:DeleteReportDefinition",
    "cur:DescribeReportDefinitions"
  ],
  "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
},
{
  "Effect" : "Allow",
  "Action" : "cur:DescribeReportDefinitions",
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDataExchangeFullAccess

AWSDataExchangeFullAccess es una [política administrada por AWS](#) que: otorga acceso total a AWS Data Exchange y a las acciones de AWS Marketplace mediante la AWS Management Console y SDK. También, proporciona un acceso selecto a los servicios relacionados que se necesitan para aprovechar Data Exchange de AWS.

Uso de la política

Puede asociar `AWSDataExchangeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de noviembre de 2019 a las 19:27 UTC
- Hora de edición: 2 de diciembre de 2021 a las 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDataExchangeProviderFullAccess

`AWSDataExchangeProviderFullAccess` es una [política administrada por AWS](#) que: brinda al proveedor de datos acceso a AWS Data Exchange y a las acciones de AWS Marketplace mediante la AWS Management Console y SDK. También, proporciona un acceso selecto a los servicios relacionados que se necesitan para aprovechar Data Exchange de AWS.

Uso de la política

Puede asociar `AWSDataExchangeProviderFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de noviembre de 2019 a las 19:27 UTC
- Hora de edición: 15 de marzo de 2022 a las 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDataExchangeReadOnly

AWSDataExchangeReadOnly es una [política administrada por AWS](#) que: concede acceso de solo lectura a AWS Data Exchange y a las acciones de AWS Marketplace que utilizan la AWS Management Console y SDK.

Uso de la política

Puede asociar AWSDataExchangeReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de noviembre de 2019 a las 19:27 UTC
- Hora de edición: 10 de mayo de 2021 a las 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDataExchangeSubscriberFullAccess

AWSDataExchangeSubscriberFullAccess es una [política administrada por AWS](#) que: concede a los suscriptores de datos acceso a AWS Data Exchange y a las acciones de AWS Marketplace que utilizan la AWS Management Console y SDK. También, proporciona un acceso selecto a los servicios relacionados que se necesitan para aprovechar Data Exchange de AWS.

Uso de la política

Puede asociar AWSDataExchangeSubscriberFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de noviembre de 2019 a las 19:27 UTC
- Hora de edición: 29 de noviembre de 2021 a las 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDataLifecycleManagerServiceRole

`AWSDataLifecycleManagerServiceRole` es una [política administrada AWS](#) que: proporciona los permisos adecuados a AWS Data Lifecycle Manager para que tome medidas con respecto a los recursos de AWS

Uso de la política

Puede asociar `AWSDataLifecycleManagerServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de julio de 2018 a las 19:34 UTC
- Hora de edición: 19 de septiembre de 2022 a las 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
```

```

    "ec2:DescribeSnapshots",
    "ec2:EnableFastSnapshotRestores",
    "ec2:DescribeFastSnapshotRestores",
    "ec2:DisableFastSnapshotRestores",
    "ec2:CopySnapshot",
    "ec2:ModifySnapshotAttribute",
    "ec2:DescribeSnapshotAttribute",
    "ec2:DescribeSnapshotTierStatus",
    "ec2:ModifySnapshotTier"
  ],
  "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.*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDataLifecycleManagerServiceRoleForAMIManagement

AWSDataLifecycleManagerServiceRoleForAMIManagement es una [política administrada por AWS](#) que: otorga los permisos adecuados a AWS Data Lifecycle Manager para que tome medidas con respecto a los recursos de AWS de la administración de la AMI

Uso de la política

Puede asociar AWSDataLifecycleManagerServiceRoleForAMIManagement a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 21 de octubre de 2020 a las 19:39 UTC
- Hora de edición: 19 de agosto de 2021 a las 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```



```
    "Resource" : [
      "arn:aws:ec2:*::snapshot/*",
      "arn:aws:ec2:*::image/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeVolumes",
      "ec2:DescribeSnapshots"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:DeleteSnapshot",
    "Resource" : "arn:aws:ec2:*::snapshot/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ResetImageAttribute",
      "ec2:DeregisterImage",
      "ec2:CreateImage",
      "ec2:CopyImage",
      "ec2:ModifyImageAttribute"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:EnableImageDeprecation",
      "ec2:DisableImageDeprecation"
    ],
    "Resource" : "arn:aws:ec2:*::image/*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDatalifecycleManagerSSMFullAccess

AWSDatalifecycleManagerSSMFullAccess es una [política administrada por AWS](#) que: brinda permiso a Amazon Data Lifecycle Manager para que realice las acciones de Systems Manager necesarias para ejecutar scripts previos y posteriores en todas las instancias de Amazon EC2.

Uso de la política

Puede asociar AWSDatalifecycleManagerSSMFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 31 de octubre de 2023 a las 20:29 UTC
- Hora editada: 16 de noviembre de 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDatalifecycleManagerSSMFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "Sid" : "AllowAllEC2Instances",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDatapipeline_FullAccess

AWSDatapipeline_FullAccess es una [política administrada por AWS](#) que: concede acceso total a Data Pipeline, acceso a listas para S3, DynamoDB, Redshift, RDS, SNS y los roles de IAM, y acceso a PassRole para los roles predeterminados.

Uso de la política

Puede asociar AWSDatapipeline_FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de enero de 2017 a las 23:14 UTC

- Hora de edición: 17 de agosto de 2017 a las 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
```

```
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
    ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDatapipeline_PowerUser

AWSDatapipeline_PowerUser es una [política administrada por AWS](#) que: proporciona acceso total a Data Pipeline, acceso a listas para S3, DynamoDB, Redshift, RDS, SNS y los roles de IAM, y acceso a PassRole para los roles predeterminados.

Uso de la política

Puede asociar AWSDatapipeline_PowerUser a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de enero de 2017 a las 23:16 UTC
- Hora de edición: 17 de agosto de 2017 a las 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDatapipeline_PowerUser`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDataSyncDiscoveryServiceRolePolicy

AWSDataSyncDiscoveryServiceRolePolicy es una [política administrada por AWS](#) que permite que DataSync Discovery se integre con otros servicios de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de marzo de 2023 a las 22:19 UTC
- Hora de edición: 20 de marzo de 2023 a las 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDataSyncFullAccess

AWSDataSyncFullAccesses una [política AWS gestionada](#) que: proporciona acceso total AWS DataSync y acceso mínimo a sus dependencias

Uso de la política

Puede asociar AWSDataSyncFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de enero de 2019 a las 19:40 UTC
- Hora editada: 16 de febrero de 2024 a las 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "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"
      ]
    }
  }
}
}

```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSDDataSyncReadOnlyAccess

AWSDDataSyncReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a la aplicación de DataSync de AWS

Uso de la política

Puede asociar AWSDDataSyncReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de enero de 2019 a las 19:18 UTC
- Hora de edición: 30 de junio de 2020 a las 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDDataSyncReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:Describe*",
        "datasync:List*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeepLensLambdaFunctionAccessPolicy

AWSDeepLensLambdaFunctionAccessPolicy es una [política administrada por AWS](#) que especifica los permisos que las funciones de lambda administrativas de DeepLens requieren y que se ejecutan en un dispositivo DeepLens

Uso de la política

Puede asociar AWSDeepLensLambdaFunctionAccessPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2017 a las 15:47 UTC
- Hora de edición: 11 de junio de 2019 a las 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*/**",
        "arn:aws:s3:::deeplens*"
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "Sid" : "DeepLensGreenGrassCloudWatchAccess",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents",
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
  },
  {
    "Sid" : "DeepLensAccess",
    "Effect" : "Allow",
    "Action" : [
      "deeplens:*"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "DeepLensKinesisVideoAccess",
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:DescribeStream",
      "kinesisvideo:CreateStream",
      "kinesisvideo:GetDataEndpoint",
      "kinesisvideo:PutMedia"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDepLensServiceRolePolicy

AWSDepLensServiceRolePolicy es una [política administrada por AWS](#) que: otorga a AWS DeepLens el acceso a los Servicios de AWS, los recursos y los roles que necesita DeepLens y sus dependencias, incluidas IoT, S3, GreenGrass y AWS Lambda.

Uso de la política

Puede asociar AWSDepLensServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de noviembre de 2017 a las 15:46 UTC
- Hora de edición: 25 de septiembre de 2019 a las 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDepLensServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Action" : [
  "iot:CreateThing",
  "iot>DeleteThing",
  "iot>DeleteThingShadow",
  "iot:DescribeThing",
  "iot:GetThingShadow",
  "iot:UpdateThing",
  "iot:UpdateThingShadow"
],
"Resource" : [
  "arn:aws:iot:*:*:thing/deeplens*"
]
},
{
  "Sid" : "DeepLensIoTCertificateAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachThingPrincipal",
    "iot:DetachThingPrincipal",
    "iot:UpdateCertificate",
    "iot>DeleteCertificate",
    "iot:DetachPrincipalPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/deeplens*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateKeysAndCertificate",
    "iot:CreatePolicy",
    "iot:CreatePolicyVersion"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
  "Effect" : "Allow",
  "Action" : [
```

```
    "iot:AttachPrincipalPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/deeplens*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "DeepLensIoTDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:GetThingShadow",
    "iot:UpdateThingShadow"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/deeplens*"
  ]
},
{
  "Sid" : "DeepLensIoTEndpointAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:DescribeEndpoint"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensAccess",
  "Effect" : "Allow",
  "Action" : [
    "deeplens:*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensS3ObjectAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
}
```

```
    "Resource" : [
      "arn:aws:s3:::deeplens*"
    ]
  },
  {
    "Sid" : "DeepLensS3Buckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:DeleteBucket",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::deeplens*"
    ]
  },
  {
    "Sid" : "DeepLensCreateS3Buckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "DeepLensIAMPassRoleAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "greengrass.amazonaws.com",
          "sagemaker.amazonaws.com"
        ]
      }
    }
  },
  {
    {
```

```
"Sid" : "DeepLensIAMLambdaPassRoleAccess",
"Effect" : "Allow",
"Action" : [
  "iam:PassRole"
],
"Resource" : [
  "arn:aws:iam::*:role/AWSDeepLens*",
  "arn:aws:iam::*:role/service-role/AWSDeepLens*"
],
"Condition" : {
  "StringEqualsIfExists" : {
    "iam:PassedToService" : "lambda.amazonaws.com"
  }
}
},
{
  "Sid" : "DeepLensGreenGrassAccess",
  "Effect" : "Allow",
  "Action" : [
    "greengrass:AssociateRoleToGroup",
    "greengrass:AssociateServiceRoleToAccount",
    "greengrass:CreateResourceDefinition",
    "greengrass:CreateResourceDefinitionVersion",
    "greengrass:CreateCoreDefinition",
    "greengrass:CreateCoreDefinitionVersion",
    "greengrass:CreateDeployment",
    "greengrass:CreateFunctionDefinition",
    "greengrass:CreateFunctionDefinitionVersion",
    "greengrass:CreateGroup",
    "greengrass:CreateGroupCertificateAuthority",
    "greengrass:CreateGroupVersion",
    "greengrass:CreateLoggerDefinition",
    "greengrass:CreateLoggerDefinitionVersion",
    "greengrass:CreateSubscriptionDefinition",
    "greengrass:CreateSubscriptionDefinitionVersion",
    "greengrass>DeleteCoreDefinition",
    "greengrass>DeleteFunctionDefinition",
    "greengrass>DeleteGroup",
    "greengrass>DeleteLoggerDefinition",
    "greengrass>DeleteSubscriptionDefinition",
    "greengrass:DisassociateRoleFromGroup",
    "greengrass:DisassociateServiceRoleFromAccount",
    "greengrass:GetAssociatedRole",
    "greengrass:GetConnectivityInfo",
```

```
"greengrass:GetCoreDefinition",
"greengrass:GetCoreDefinitionVersion",
"greengrass:GetDeploymentStatus",
"greengrass:GetDeviceDefinition",
"greengrass:GetDeviceDefinitionVersion",
"greengrass:GetFunctionDefinition",
"greengrass:GetFunctionDefinitionVersion",
"greengrass:GetGroup",
"greengrass:GetGroupCertificateAuthority",
"greengrass:GetGroupCertificateConfiguration",
"greengrass:GetGroupVersion",
"greengrass:GetLoggerDefinition",
"greengrass:GetLoggerDefinitionVersion",
"greengrass:GetResourceDefinition",
"greengrass:GetServiceRoleForAccount",
"greengrass:GetSubscriptionDefinition",
"greengrass:GetSubscriptionDefinitionVersion",
"greengrass:ListCoreDefinitionVersions",
"greengrass:ListCoreDefinitions",
"greengrass:ListDeployments",
"greengrass:ListDeviceDefinitionVersions",
"greengrass:ListDeviceDefinitions",
"greengrass:ListFunctionDefinitionVersions",
"greengrass:ListFunctionDefinitions",
"greengrass:ListGroupCertificateAuthorities",
"greengrass:ListGroupVersions",
"greengrass:ListGroups",
"greengrass:ListLoggerDefinitionVersions",
"greengrass:ListLoggerDefinitions",
"greengrass:ListSubscriptionDefinitionVersions",
"greengrass:ListSubscriptionDefinitions",
"greengrass:ResetDeployments",
"greengrass:UpdateConnectivityInfo",
"greengrass:UpdateCoreDefinition",
"greengrass:UpdateDeviceDefinition",
"greengrass:UpdateFunctionDefinition",
"greengrass:UpdateGroup",
"greengrass:UpdateGroupCertificateConfiguration",
"greengrass:UpdateLoggerDefinition",
"greengrass:UpdateSubscriptionDefinition",
"greengrass:UpdateResourceDefinition"
],
"Resource" : [
  "*"
]
```

```
]
},
{
  "Sid" : "DeepLensLambdaAdminFunctionAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda>ListFunctions",
    "lambda>ListVersionsByFunction",
    "lambda:PublishVersion",
    "lambda:UpdateFunctionCode",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:deeplens*"
  ]
},
{
  "Sid" : "DeepLensLambdaUsersFunctionAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda>ListFunctions",
    "lambda>ListVersionsByFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:*"
  ]
},
{
  "Sid" : "DeepLensSageMakerWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateTrainingJob",
    "sagemaker:DescribeTrainingJob",
    "sagemaker:StopTrainingJob"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:training-job/deeplens*"
  ]
}
```

```
    },
    {
      "Sid" : "DeepLensSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo>DeleteStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeepRacerAccountAdminAccess

AWSDeepRacerAccountAdminAccess es una [política administrada por AWS](#) que: el administrador de DeepRacer accede a todas las acciones, incluida la posibilidad de alternar entre el modo multiusuario y el modo de usuario único.

Uso de la política

Puede asociar AWSDeepRacerAccountAdminAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de octubre de 2021 a las 01:27 UTC
- Hora de edición: 28 de octubre de 2021 a las 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
    "deeperacer:*"  
  ],  
  "Resource" : [  
    "*" ]  
  ],  
  "Condition" : {  
    "Null" : {  
      "deeperacer:UserToken" : "true"  
    }  
  }  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeepRacerCloudFormationAccessPolicy

AWSDeepRacerCloudFormationAccessPolicy es una [política administrada por AWS](#) que: permite que CloudFormation cree y gestione pilas de AWS y recursos en su nombre.

Uso de la política

Puede asociar AWSDeepRacerCloudFormationAccessPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de febrero de 2019 a las 21:59 UTC
- Hora de edición: 14 de junio de 2019 a las 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteInternetGateway",
        "ec2>DeleteNatGateway",
        "ec2>DeleteNetworkAcl",
        "ec2>DeleteNetworkAclEntry",
```

```
    "ec2:DeleteRoute",
    "ec2:DeleteRouteTable",
    "ec2:DeleteSecurityGroup",
    "ec2:DeleteSubnet",
    "ec2:DeleteTags",
    "ec2:DeleteVpc",
    "ec2:DeleteVpcEndpoints",
    "ec2:DescribeAddresses",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTags",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcs",
    "ec2:DetachInternetGateway",
    "ec2:DisassociateRouteTable",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:ReleaseAddress",
    "ec2:ReplaceNetworkAclAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
  "Condition" : {
    "StringLikeIfExists" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
```

```

    "lambda:GetFunction",
    "lambda:DeleteFunction",
    "lambda:TagResource",
    "lambda:UpdateFunctionCode"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:*DeepRacer*",
    "arn:aws:lambda:*:*:function:*Deepracer*",
    "arn:aws:lambda:*:*:function:*deepracer*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketPolicy",
    "s3:CreateBucket",
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3>DeleteBucket"
  ],
  "Resource" : [
    "arn:aws:s3::*:*DeepRacer*",
    "arn:aws:s3::*:*Deepracer*",
    "arn:aws:s3::*:*deepracer*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "robomaker:CreateSimulationApplication",
    "robomaker:CreateSimulationApplicationVersion",
    "robomaker>DeleteSimulationApplication",
    "robomaker:DescribeSimulationApplication",
    "robomaker>ListSimulationApplications",
    "robomaker:TagResource",
    "robomaker:UpdateSimulationApplication"
  ],
  "Resource" : [
    "arn:aws:robomaker:*:*:/createSimulationApplication",
    "arn:aws:robomaker:*:*:simulation-application/deepracer*"
  ]
}
]

```

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeepRacerDefaultMultiUserAccess

AWSDeepRacerDefaultMultiUserAccess es una [política administrada por AWS](#) que: concede a DeepRacer MultiUser acceso de usuario predeterminado para usar DeepRacer en modo multiusuario

Uso de la política

Puede asociar AWSDeepRacerDefaultMultiUserAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de octubre de 2021 a las 01:27 UTC
- Hora de edición: 28 de octubre de 2021 a las 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer>Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer>Delete*",
        "deepracer:Stop*",
        "deepracer:Import*",
        "deepracer:Tag*",
        "deepracer:Untag*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "false"
        },
        "Bool" : {
          "deepracer:MultiUser" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:GetAccountConfig",
        "deepracer:GetTrack",
        "deepracer:ListTracks",

```

```
    "deepracer:TestRewardFunction"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "deepracer:Admin*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeepRacerFullAccess

AWSDeepRacerFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a AWS DeepRacer. También, brinda acceso selecto a servicios relacionados (por ejemplo, S3).

Uso de la política

Puede asociar AWSDeepRacerFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de octubre de 2020 a las 22:03 UTC
- Hora de edición: 5 de octubre de 2020 a las 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ]
    }
  ]
}
```



```
    ],
    "Resource" : [
        "arn:aws:s3::*DeepRacer*",
        "arn:aws:s3::*Deepracer*",
        "arn:aws:s3::*deepracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3::*DeepRacer/*",
        "arn:aws:s3::*Deepracer/*",
        "arn:aws:s3::*deepracer/*",
        "arn:aws:s3:::dr-*/*"
    ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeepRacerRoboMakerAccessPolicy

AWSDeepRacerRoboMakerAccessPolicy es una [política administrada por AWS](#) que: permite que RoboMaker cree los recursos necesarios y llame a los servicios de AWS en su nombre.

Uso de la política

Puede asociar AWSDeepRacerRoboMakerAccessPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de febrero de 2019 a las 21:59 UTC
- Hora de edición: 28 de febrero de 2019 a las 21:59 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:PutObject"
    ],
    "Resource" : [
        "arn:aws:s3::*DeepRacer*",
        "arn:aws:s3::*Deepracer*",
        "arn:aws:s3::*deepracer*",
        "arn:aws:s3::*dr-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEqualsIgnoreCase" : {
            "s3:ExistingObjectTag/DeepRacer" : "true"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
    ],
    "Resource" : [

```

```
        "arn:aws:kinesisvideo:*:*:stream/dr-*"  
    ]  
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeepRacerServiceRolePolicy

AWSDeepRacerServiceRolePolicy es una [política administrada por AWS](#) que: permite que DeepRacer cree los recursos necesarios y llame a los servicios de AWS en su nombre.

Uso de la política

Puede asociar AWSDeepRacerServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de febrero de 2019 a las 21:58 UTC
- Hora de edición: 12 de junio de 2019 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*",
        "sagemaker:*",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DetectStackDrift",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackResourceDrifts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : "iam:CreateServiceLinkedRole",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "robomaker.amazonaws.com"
      }
    },
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AWSDeepRacer*",
      "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:GetLogEvents",
      "logs:PutLogEvents"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:GetFunction",
      "lambda:InvokeFunction",
      "lambda:UpdateFunctionCode"
    ],
    "Resource" : [
      "arn:aws:lambda::*:function:*DeepRacer*",
      "arn:aws:lambda::*:function:*Deepracer*",
      "arn:aws:lambda::*:function:*deepracer*",
      "arn:aws:lambda::*:function:*dr-*"
    ]
  }
}

```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetBucketLocation",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutBucketPolicy",
    "s3:GetBucketAcl"
  ],
  "Resource" : [
    "arn:aws:s3::*DeepRacer*",
    "arn:aws:s3::*Deepracer*",
    "arn:aws:s3::*deepracer*",
    "arn:aws:s3:::dr-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/DeepRacer" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kinesisvideo:CreateStream",
    "kinesisvideo>DeleteStream",
    "kinesisvideo:DescribeStream",
    "kinesisvideo:GetDataEndpoint",
    "kinesisvideo:GetHLSStreamingSessionURL",
    "kinesisvideo:GetMedia",
    "kinesisvideo:PutMedia",
    "kinesisvideo:TagStream"
  ],
}
```

```
    "Resource" : [  
      "arn:aws:kinesisvideo:*:*:stream/dr-*"  
    ]  
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDenyAll

AWSDenyAll esta es una [política administrada por AWS](#) que: deniega el acceso.

Uso de la política

Puede asociar AWSDenyAll a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de mayo de 2019 a las 22:36 UTC
- Hora editada: 18 de diciembre de 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeviceFarmFullAccess

AWSDeviceFarmFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todas las operaciones de AWS Device Farm.

Uso de la política

Puede asociar AWSDeviceFarmFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de julio de 2015 a las 16:37 UTC
- Hora de edición: 13 de julio de 2015 a las 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeviceFarmServiceRolePolicy

AWSDeviceFarmServiceRolePolicy es una [política administrada por AWS](#) que: concede permisos a AWS Device Farm para que llame a las API de red de EC2 en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de septiembre de 2022 a las 21:02 UTC
- Hora de edición: 20 de septiembre de 2022 a las 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ]
    }
  ],
}
```

```

    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/AWSDeviceFarmManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface"
    ],
  },

```

```
"Resource" : "arn:aws:ec2:*:*:network-interface/*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDeviceFarmTestGridServiceRolePolicy

AWSDeviceFarmTestGridServiceRolePolicy es una [política administrada por AWS](#) que: concede permisos a AWS Device Farm para que llame a las API de EC2 en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de mayo de 2021 a las 22:01 UTC
- Hora de edición: 26 de mayo de 2021 a las 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ]
    }
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/AWSDeviceFarmManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface"
    ],
  },
```

```
"Resource" : "arn:aws:ec2:*:*:network-interface/*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess` es una [política administrada por AWS](#) que: proporciona acceso total a AWS Direct Connect a través de la AWS Management Console.

Uso de la política

Puede asociar `AWSDirectConnectFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 30 de abril de 2019 a las 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDirectConnectReadOnlyAccess

`AWSDirectConnectReadOnlyAccess` es una [política administrada por AWS](#) que: Proporciona acceso de solo lectura a AWS Direct Connect a través de la AWS Management Console.

Uso de la política

Puede asociar `AWSDirectConnectReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 18 de mayo de 2020 a las 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDirectConnectServiceRolePolicy

AWSDirectConnectServiceRolePolicy es una [política administrada por AWS](#) que: brinda permiso a AWS Direct Connect para crear y administrar recursos de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de enero de 2021 a las 18:35 UTC
- Hora de edición: 14 de enero de 2021 a las 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDirectoryServiceFullAccess

AWSDirectoryServiceFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS Directory Service.

Uso de la política

Puede asociar AWSDirectoryServiceFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 24 de noviembre de 2020 a las 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDirectoryServiceReadOnlyAccess

AWSDirectoryServiceReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a AWS Directory Service.

Uso de la política

Puede asociar AWSDirectoryServiceReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 25 de septiembre de 2018 a las 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDiscoveryContinuousExportFirehosePolicy

AWSDiscoveryContinuousExportFirehosePolicy es una [política administrada por AWS](#) que: otorga acceso de escritura a los recursos de AWS necesarios para AWS Discovery Continuous Export

Uso de la política

Puede asociar AWSDiscoveryContinuousExportFirehosePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de agosto de 2018 a las 18:29 UTC
- Hora de edición: 8 de junio de 2021 a las 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-application-discovery-service-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-
stream:*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDMSFleetAdvisorServiceRolePolicy

AWSDMSFleetAdvisorServiceRolePolicy es una [política administrada por AWS](#) que: permite que DMS Fleet Advisor gestione las métricas de CloudWatch en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de marzo de 2023 a las 09:10 UTC
- Hora de edición: 6 de marzo de 2023 a las 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSDMSServerlessServiceRolePolicy

AWSDMSServerlessServiceRolePolicy es una [política administrada por AWS](#) que: otorga a DMS de AWS permisos sin servidor para que cree y administre los recursos de DMS en su cuenta en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de mayo de 2023 a las 20:28 UTC
- Hora de edición: 18 de mayo de 2023 a las 20:28 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
```

```

    "Action" : [
      "dms:StartReplicationTask",
      "dms:StopReplicationTask",
      "dms>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:*"
    ]
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSEC2CapacityReservationFleetRolePolicy

AWSEC2CapacityReservationFleetRolePolicy es una [política administrada por AWS](#) que permite que el servicio CapacityReservation Fleet de EC2 gestione las reservas de capacidad

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de septiembre de 2021 a las 14:43 UTC
- Hora de edición: 29 de septiembre de 2021 a las 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
```

```

        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
    ],
    "Condition" : {
        "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"
        }
    }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSEC2FleetServiceRolePolicy

AWSEC2FleetServiceRolePolicy es una [política administrada por AWS](#) que: permite que EC2 Fleet lance y gestione instancias.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de marzo de 2018 a las 00:08 UTC
- Hora de edición: 4 de mayo de 2020 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
  ],
}
```

```
"Sid" : "EC2SpotManagement",
"Effect" : "Allow",
"Action" : [
  "iam:CreateServiceLinkedRole"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:AWSServiceName" : "spot.amazonaws.com"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:spot-instances-request/*"
  ]
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
}
```

```
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSEC2SpotFleetServiceRolePolicy

AWSEC2SpotFleetServiceRolePolicy es una [política administrada por AWS](#) que: permite que la Flota de sport de EC2 lance y gestione instancias de flota de spot puntual

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de octubre de 2017 a las 19:13 UTC
- Hora de edición: 16 de marzo de 2020 a las 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```

    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:spot-instances-request/*",
    "arn:aws:ec2:*:*:spot-fleet-request/*",
    "arn:aws:ec2:*:*:volume*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
  ],
  "Resource" : [
    "arn:aws:elasticloadbalancing:*:*:loadbalancer*"
  ]
},

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterTargets"
  ],
  "Resource" : [
    "arn:aws:elasticloadbalancing:*:*:*/*"
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSEC2SpotServiceRolePolicy

AWSEC2SpotServiceRolePolicy es una [política administrada por AWS](#) que: permite que EC2 Spot lance y gestione instancias puntuales

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de septiembre de 2017 a las 18:51 UTC
- Hora de edición: 12 de diciembre de 2018 a las 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "ec2:InstanceMarketType" : "spot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSECRPullThroughCache_ServiceRolePolicy

AWSECRPullThroughCache_ServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los servicios y recursos de AWS utilizados o gestionados por la memoria caché de extracción de AWS ECR

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2021 a las 21:51 UTC
- Hora de edición: 13 de noviembre de 2023 a las 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

AWSElasticBeanstalkCustomPlatformforEC2Role es una [política administrada por AWS](#) que: brinda permiso a la instancia de su entorno de creación de plataformas personalizado para que lance una instancia EC2, cree una instantánea y una AMI de EBS, transmita registros a los Registros de Amazon CloudWatch y almacene artefactos en Amazon S3.

Uso de la política

Puede asociar AWSElasticBeanstalkCustomPlatformforEC2Role a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de febrero de 2017 a las 22:50 UTC
- Hora de edición: 21 de febrero de 2017 a las 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Access",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateKeypair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2>DeleteKeypair",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteSnapshot",
        "ec2>DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:GetPasswordData",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySnapshotAttribute",
        "ec2:RegisterImage",
        "ec2:RunInstances",
        "ec2:StopInstances",
```

```
    "ec2:TerminateInstances"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "BucketAccess",
  "Action" : [
    "s3:Get*",
    "s3:List*",
    "s3:PutObject"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:s3:::elasticbeanstalk-*",
    "arn:aws:s3:::elasticbeanstalk-*/*"
  ]
},
{
  "Sid" : "CloudWatchLogsAccess",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkEnhancedHealth

AWSElasticBeanstalkEnhancedHealth es una [política administrada por AWS](#) que: es una política de AWS Elastic Beanstalk Service para el sistema Health Monitoring

Uso de la política

Puede asociar AWSElasticBeanstalkEnhancedHealth a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 8 de febrero de 2016 a las 23:17 UTC
- Hora de edición: 9 de abril de 2018 a las 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:GetConsoleOutput",
        "ec2:AssociateAddress",
```

```
    "ec2:DescribeAddresses",
    "ec2:DescribeSecurityGroups",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:DescribeNotificationConfigurations",
    "sns:Publish"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkMaintenance

AWSElasticBeanstalkMaintenance es una [política administrada por AWS](#) que: es una política de rol de servicio de AWS Elastic Beanstalk que otorga permisos limitados para actualizar sus recursos en su nombre con fines de mantenimiento.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 11 de enero de 2019 a las 23:22 UTC
- Hora de edición: 4 de junio de 2019 a las 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy es una [política administrada por AWS](#) que: es para el rol de servicio de AWS Elastic Beanstalk que se utiliza para realizar actualizaciones gestionadas de los entornos de Elastic Beanstalk. Esta política no debe asociarse a otros usuarios o roles. La política otorga amplios permisos para crear y administrar recursos en varios servicios de AWS, incluidos AutoScaling, EC2, ECS, Elastic Load Balancing y CloudFormation. Esta política también permite transferir cualquier rol de IAM que pueda utilizarse con esos servicios.

Uso de la política

Puede asociar AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de marzo de 2021 a las 22:18 UTC
- Hora de edición: 23 de marzo de 2023 a las 23:15 UTC

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

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
},
{
  "Sid" : "ReadOnlyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DescribeAccountLimits",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeLoadBalancers",
    "autoscaling:DescribeNotificationConfigurations",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:DescribeScheduledActions",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcClassicLink",
    "ec2:DescribeVpcs",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "logs:DescribeLogGroups",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeOrderableDBInstanceOptions",
    "sns:ListSubscriptionsByTopic"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2BroadOperationPermissions",
```

```

"Effect" : "Allow",
"Action" : [
  "ec2:AllocateAddress",
  "ec2:AssociateAddress",
  "ec2:AuthorizeSecurityGroupEgress",
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2:CreateLaunchTemplate",
  "ec2:CreateLaunchTemplateVersion",
  "ec2:CreateSecurityGroup",
  "ec2>DeleteLaunchTemplate",
  "ec2>DeleteLaunchTemplateVersions",
  "ec2>DeleteSecurityGroup",
  "ec2:DisassociateAddress",
  "ec2:ReleaseAddress",
  "ec2:RevokeSecurityGroupEgress",
  "ec2:RevokeSecurityGroupIngress"
],
"Resource" : "*"
},
{
  "Sid" : "EC2RunInstancesOperationPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "EC2TerminateInstancesOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    }
  }
}

```

```

    }
  },
  {
    "Sid" : "ECSBroadOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ecs:CreateCluster",
      "ecs:DescribeClusters",
      "ecs:RegisterTaskDefinition"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ECSDeleteClusterOperationPermissions",
    "Effect" : "Allow",
    "Action" : "ecs:DeleteCluster",
    "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
  },
  {
    "Sid" : "ASGOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling:CreateOrUpdateTags",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteScheduledAction",
      "autoscaling:DetachInstances",
      "autoscaling>DeletePolicy",
      "autoscaling:PutScalingPolicy",
      "autoscaling:PutScheduledUpdateGroupAction",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:ResumeProcesses",
      "autoscaling:SetDesiredCapacity",
      "autoscaling:SuspendProcesses",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "autoscaling:UpdateAutoScalingGroup"
    ],
    "Resource" : [
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",

```

```

        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
    ]
},
{
    "Sid" : "CFNOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
        "cloudformation:*"
    ],
    "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
    ]
},
{
    "Sid" : "ELBOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing>CreateLoadBalancer",
        "elasticloadbalancing>DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/**",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/**"
    ]
},
{
    "Sid" : "CWLogsOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",

```

```
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
},
{
  "Sid" : "S3ObjectOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionAcl",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutObjectVersionAcl"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
},
{
  "Sid" : "S3BucketOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy",
    "s3:ListBucket",
    "s3:PutBucketPolicy"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
},
{
  "Sid" : "SNSOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:GetTopicAttributes",
    "sns:SetTopicAttributes",
    "sns:Subscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
},
{
  "Sid" : "SQSOperationPermissions",
  "Effect" : "Allow",
```

```

    "Action" : [
      "sqs:GetQueueAttributes",
      "sqs:GetQueueUrl"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:awseb-e-*",
      "arn:aws:sqs:*:*:eb-*"
    ]
  },
  {
    "Sid" : "CWPutMetricAlarmOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : [
      "arn:aws:cloudwatch:*:*:alarm:awseb-*",
      "arn:aws:cloudwatch:*:*:alarm:eb-*"
    ]
  },
  {
    "Sid" : "AllowECSTagResource",
    "Effect" : "Allow",
    "Action" : [
      "ecs:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "CreateCluster",
          "RegisterTaskDefinition"
        ]
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy es una [política administrada por AWS](#) que: es una política de rol de servicio de AWS Elastic Beanstalk que otorga permisos limitados a las actualizaciones gestionadas.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de noviembre de 2019 a las 22:35 UTC
- Hora de edición: 24 de marzo de 2023 a las 00:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
{
  "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringLikeIfExists" : {
      "iam:PassedToService" : [
        "elasticbeanstalk.amazonaws.com",
        "ec2.amazonaws.com",
        "autoscaling.amazonaws.com",
        "elasticloadbalancing.amazonaws.com",
        "ecs.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "SingleInstanceAPIs",
  "Effect" : "Allow",
  "Action" : [
    "ec2:releaseAddress",
    "ec2:allocateAddress",
    "ec2:DisassociateAddress",
    "ec2:AssociateAddress"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ECS",
  "Effect" : "Allow",
  "Action" : [
    "ecs:RegisterTaskDefinition",
    "ecs:DeRegisterTaskDefinition",
    "ecs:List*",
    "ecs:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ElasticBeanstalkAPIs",
  "Effect" : "Allow",
  "Action" : [
```

```

    "elasticbeanstalk:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ReadOnlyAPIs",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:Describe*",
    "cloudformation:List*",
    "ec2:Describe*",
    "autoscaling:Describe*",
    "elasticloadbalancing:Describe*",
    "logs:DescribeLogGroups",
    "sns:GetTopicAttributes",
    "sns:ListSubscriptionsByTopic",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ASG",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling:CreateOrUpdateTags",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling>DeleteScheduledAction",
    "autoscaling:DetachInstances",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:PutScalingPolicy",
    "autoscaling:PutScheduledUpdateGroupAction",
    "autoscaling:ResumeProcesses",
    "autoscaling:SuspendProcesses",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup"
  ],
  "Resource" : [
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
**",

```

```

    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
  ]
},
{
  "Sid" : "CFN",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:CancelUpdateStack",
    "cloudformation>DeleteStack",
    "cloudformation:GetTemplate",
    "cloudformation:UpdateStack"
  ],
  "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"
      ]
    }
  }
}
```

```
}  
  ]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkMulticontainerDocker

AWSElasticBeanstalkMulticontainerDocker es una [política administrada por AWS](#) que: proporciona acceso a las instancias de su entorno Docker multicontenedor para utilizar EC2 Container Service de Amazon a fin de gestionar las tareas de implementación de contenedores.

Uso de la política

Puede asociar AWSElasticBeanstalkMulticontainerDocker a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de febrero de 2016 a las 23:15 UTC
- Hora de edición: 23 de marzo de 2023 a las 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "ECSAccess",
    "Effect" : "Allow",
    "Action" : [
      "ecs:Poll",
      "ecs:StartTask",
      "ecs:StopTask",
      "ecs:DiscoverPollEndpoint",
      "ecs:StartTelemetrySession",
      "ecs:RegisterContainerInstance",
      "ecs:DeregisterContainerInstance",
      "ecs:DescribeContainerInstances",
      "ecs:Submit*",
      "ecs:DescribeTasks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowECSTagResource",
    "Effect" : "Allow",
    "Action" : [
      "ecs:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "RegisterContainerInstance",
          "StartTask"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkReadOnly

AWSElasticBeanstalkReadOnly es una [política administrada por AWS](#) que: concede permisos de solo lectura. Permite explícitamente que los operadores obtengan acceso directo para recuperar información sobre los recursos relacionados con las aplicaciones de AWS Elastic Beanstalk.

Uso de la política

Puede asociar AWSElasticBeanstalkReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de enero de 2021 a las 19:02 UTC
- Hora de edición: 22 de enero de 2021 a las 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Action" : [  
  "acm:ListCertificates",  
  "autoscaling:DescribeAccountLimits",  
  "autoscaling:DescribeAutoScalingGroups",  
  "autoscaling:DescribeAutoScalingInstances",  
  "autoscaling:DescribeLaunchConfigurations",  
  "autoscaling:DescribePolicies",  
  "autoscaling:DescribeLoadBalancers",  
  "autoscaling:DescribeNotificationConfigurations",  
  "autoscaling:DescribeScalingActivities",  
  "autoscaling:DescribeScheduledActions",  
  "cloudformation:DescribeStackResource",  
  "cloudformation:DescribeStackResources",  
  "cloudformation:DescribeStacks",  
  "cloudformation:GetTemplate",  
  "cloudformation:ListStackResources",  
  "cloudformation:ListStacks",  
  "cloudformation:ValidateTemplate",  
  "cloudtrail:LookupEvents",  
  "cloudwatch:DescribeAlarms",  
  "cloudwatch:GetMetricStatistics",  
  "cloudwatch:ListMetrics",  
  "ec2:DescribeAccountAttributes",  
  "ec2:DescribeAddresses",  
  "ec2:DescribeImages",  
  "ec2:DescribeInstanceAttribute",  
  "ec2:DescribeInstances",  
  "ec2:DescribeInstanceStatus",  
  "ec2:DescribeKeyPairs",  
  "ec2:DescribeLaunchTemplateVersions",  
  "ec2:DescribeLaunchTemplates",  
  "ec2:DescribeSecurityGroups",  
  "ec2:DescribeSnapshots",  
  "ec2:DescribeSpotInstanceRequests",  
  "ec2:DescribeAvailabilityZones",  
  "ec2:DescribeSubnets",  
  "ec2:DescribeVpcs",  
  "elasticbeanstalk:Check*",  
  "elasticbeanstalk:Describe*",  
  "elasticbeanstalk:List*",  
  "elasticbeanstalk:RequestEnvironmentInfo",  
  "elasticbeanstalk:RetrieveEnvironmentInfo",  
  "elasticloadbalancing:DescribeInstanceHealth",  
  "elasticloadbalancing:DescribeLoadBalancers",
```

```

    "elasticloadbalancing:DescribeSSLPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "iam:GetRole",
    "iam:ListAttachedRolePolicies",
    "iam:ListInstanceProfiles",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListServerCertificates",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribeDBSnapshots",
    "s3:ListAllMyBuckets",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowS3",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionAcl",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy",
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkRoleCore

AWSElasticBeanstalkRoleCore es una [política administrada por AWS](#) que:

AWSElasticBeanstalkRoleCore (rol de operaciones de Elastic Beanstalk) permite el funcionamiento principal de un entorno de servicios web.

Uso de la política

Puede asociar AWSElasticBeanstalkRoleCore a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:48 UTC
- Hora de edición: 9 de septiembre de 2020 a las 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "ec2:TerminateInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/awseb-e-*"
    }
  }
},
{
  "Sid" : "EC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ReleaseAddress",
    "ec2:AllocateAddress",
    "ec2:DisassociateAddress",
    "ec2:AssociateAddress",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteSecurityGroup",
    "ec2:AuthorizeSecurityGroup*",
    "ec2:RevokeSecurityGroup*",
    "ec2:CreateLaunchTemplate*",
    "ec2>DeleteLaunchTemplate*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LTRunInstances",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "ASG",
  "Effect" : "Allow",
  "Action" : [

```

```

    "autoscaling:AttachInstances",
    "autoscaling:*LoadBalancer*",
    "autoscaling:*AutoScalingGroup",
    "autoscaling:*LaunchConfiguration",
    "autoscaling:DeleteScheduledAction",
    "autoscaling:DetachInstances",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:PutScalingPolicy",
    "autoscaling:PutScheduledUpdateGroupAction",
    "autoscaling:ResumeProcesses",
    "autoscaling:SuspendProcesses",
    "autoscaling:*Tags"
  ],
  "Resource" : [
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
  ]
},
{
  "Sid" : "ASGPolicy",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DeletePolicy"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EBSLR",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
    }
  }
}
}

```

```
  },
  {
    "Sid" : "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"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkRoleCWL

AWSElasticBeanstalkRoleCWL es una [política administrada por AWS](#) por la que: (el rol de operaciones de Elastic Beanstalk) permite que un entorno gestione los grupos de registros de los Registros de Amazon CloudWatch.

Uso de la política

Puede asociar `AWSElasticBeanstalkRoleCWL` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:49 UTC
- Hora de edición: 5 de junio de 2020 a las 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkRoleECS

AWSElasticBeanstalkRoleECS es una [política administrada por AWS](#) por la que: (el rol de operaciones de Elastic Beanstalk) permite que un entorno Docker multicontenedor administre los clústeres de Amazon ECS.

Uso de la política

Puede asociar AWSElasticBeanstalkRoleECS a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:47 UTC
- Hora de edición: 23 de marzo de 2023 a las 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AllowECS",
    "Effect" : "Allow",
    "Action" : [
      "ecs:CreateCluster",
      "ecs>DeleteCluster",
      "ecs:RegisterTaskDefinition",
      "ecs:DeRegisterTaskDefinition"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AllowECSTagResource",
    "Effect" : "Allow",
    "Action" : [
      "ecs:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "CreateCluster",
          "RegisterTaskDefinition"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkRoleRDS

AWSElasticBeanstalkRoleRDS es una [política administrada por AWS](#) por la que: (el rol de operaciones de Elastic Beanstalk) permite que un entorno integre una instancia de Amazon RDS.

Uso de la política

Puede asociar AWSElasticBeanstalkRoleRDS a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:46 UTC
- Hora de edición: 5 de junio de 2020 a las 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "rds:DeleteDBSecurityGroup",
    "rds:AuthorizeDBSecurityGroupIngress",
    "rds:CreateDBInstance",
    "rds:ModifyDBInstance",
    "rds>DeleteDBInstance"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:secgrp:awseb-e-*",
    "arn:aws:rds:*:*:db:*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkRoleSNS

AWSElasticBeanstalkRoleSNS es una [política administrada por AWS](#) por la que: (el rol de operaciones de Elastic Beanstalk) permite que un entorno active la integración de temas de Amazon SNS.

Uso de la política

Puede asociar AWSElasticBeanstalkRoleSNS a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:46 UTC
- Hora de edición: 5 de junio de 2020 a las 21:46 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBeanstalkManageSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns>DeleteTopic"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
      ]
    },
    {
      "Sid" : "AllowSNSPublish",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkRoleWorkerTier

AWSElasticBeanstalkRoleWorkerTier es una [política administrada por AWS](#) que: (el rol de operaciones de Elastic Beanstalk) permite que un nivel de entorno de trabajo cree una tabla de Amazon DynamoDB y una cola de Amazon SQS.

Uso de la política

Puede asociar AWSElasticBeanstalkRoleWorkerTier a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:43 UTC
- Hora de edición: 5 de junio de 2020 a las 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs>DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs>CreateQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
    },
    {
      "Sid" : "AllowDDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb>CreateTable",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb>DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkService

AWSElasticBeanstalkService es una [política administrada por AWS](#) que: está en vías de caducar. Consulte la documentación para orientarse: <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>. AWS La política de roles de servicio de Elastic Beanstalk otorga permisos para crear y administrar recursos (por ejemplo, AutoScaling, EC2, S3, CloudFormation, ELB, etc.) en su nombre.

Uso de la política

Puede asociar AWSElasticBeanstalkService a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de abril de 2016 a las 20:27 UTC
- Hora de edición: 10 de mayo de 2023 a las 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Versión de la política

Versión de la política: v17 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "arn:aws:cloudformation:*:*:stack/awseb-*",
    "arn:aws:cloudformation:*:*:stack/eb-*"
  ]
},
{
  "Sid" : "AllowDeleteCloudwatchLogGroups",
  "Effect" : "Allow",
  "Action" : [
    "logs:DeleteLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
  ]
},
{
  "Sid" : "AllowECSTagResource",
  "Effect" : "Allow",
  "Action" : [
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:CreateAction" : [
        "CreateCluster",
        "RegisterTaskDefinition"
      ]
    }
  }
},
{
  "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:*"
  ],
  "Resource" : [
    "arn:aws:s3:::elasticbeanstalk-*",
    "arn:aws:s3:::elasticbeanstalk-*/*"
  ]
},
{
  "Sid" : "AllowLaunchTemplateRunInstances",
  "Effect" : "Allow",

```

```

    "Action" : "ec2:RunInstances",
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
      }
    }
  },
  {
    "Sid" : "AllowELBAddTags",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "elasticloadbalancing:CreateAction" : [
          "CreateLoadBalancer"
        ]
      }
    }
  },
  {
    "Sid" : "AllowOperations",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling:CreateOrUpdateTags",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteScheduledAction",
      "autoscaling:DescribeAccountLimits",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribeAutoScalingInstances",
      "autoscaling:DescribeLaunchConfigurations",
      "autoscaling:DescribeLoadBalancers",
      "autoscaling:DescribeNotificationConfigurations",
      "autoscaling:DescribeScalingActivities",
      "autoscaling:DescribeScheduledActions",
      "autoscaling:DetachInstances",
      "autoscaling>DeletePolicy",

```

```
"autoscaling:PutScalingPolicy",
"autoscaling:PutScheduledUpdateGroupAction",
"autoscaling:PutNotificationConfiguration",
"autoscaling:ResumeProcesses",
"autoscaling:SetDesiredCapacity",
"autoscaling:SuspendProcesses",
"autoscaling:TerminateInstanceInAutoScalingGroup",
"autoscaling:UpdateAutoScalingGroup",
"cloudwatch:PutMetricAlarm",
"ec2:AssociateAddress",
"ec2:AllocateAddress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateLaunchTemplate",
"ec2:CreateLaunchTemplateVersion",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeLaunchTemplateVersions",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteLaunchTemplateVersions",
"ec2:CreateSecurityGroup",
"ec2>DeleteSecurityGroup",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeImages",
"ec2:DescribeInstances",
"ec2:DescribeKeyPairs",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeVpcClassicLink",
"ec2:DisassociateAddress",
"ec2:ReleaseAddress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:TerminateInstances",
"ecs:CreateCluster",
"ecs>DeleteCluster",
"ecs:DescribeClusters",
"ecs:RegisterTaskDefinition",
"elasticbeanstalk:*",
"elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
```

```
"elasticloadbalancing:ConfigureHealthCheck",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing>DeleteLoadBalancer",
"elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:DeregisterTargets",
"iam:ListRoles",
"iam:PassRole",
"logs:CreateLogGroup",
"logs:PutRetentionPolicy",
"logs:DescribeLogGroups",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeOrderableDBInstanceOptions",
"s3:GetObject",
"s3:GetObjectAcl",
"s3:ListBucket",
"sns:CreateTopic",
"sns:GetTopicAttributes",
"sns:ListSubscriptionsByTopic",
"sns:Subscribe",
"sns:SetTopicAttributes",
"sqs:GetQueueAttributes",
"sqs:GetQueueUrl",
"codebuild:CreateProject",
"codebuild>DeleteProject",
"codebuild:BatchGetBuilds",
"codebuild:StartBuild"
],
"Resource" : [
  "*"
]
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkServiceRolePolicy

AWSElasticBeanstalkServiceRolePolicy es una [política administrada por AWS](#) que: es una política de AWS de roles vinculados a un servicio de Elastic Beanstalk que otorga permisos para crear y administrar recursos (por ejemplo, AutoScaling, EC2, S3, CloudFormation, ELB, etc.) en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de septiembre de 2017 a las 23:46 UTC
- Hora de edición: 6 de junio de 2019 a las 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:PutNotificationConfiguration",
        "ec2:DescribeInstanceStatus",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "lambda:GetFunction",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "Sid" : "AllowOperationsOnHealthStreamingLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs>DeleteLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkWebTier

AWSElasticBeanstalkWebTier es una [política administrada por AWS](#) que: proporciona a las instancias de su entorno de servidor web acceso para cargar archivos de registro en Amazon S3.

Uso de la política

Puede asociar AWSElasticBeanstalkWebTier a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de febrero de 2016 a las 23:08 UTC
- Hora de edición: 9 de septiembre de 2020 a las 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",

```

```
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
  ]
},
{
  "Sid" : "ElasticBeanstalkHealthAccess",
  "Action" : [
    "elasticbeanstalk:PutInstanceStatistics"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:elasticbeanstalk:*:*:application/*",
    "arn:aws:elasticbeanstalk:*:*:environment/*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticBeanstalkWorkerTier

AWSElasticBeanstalkWorkerTier es una [política administrada por AWS](#) que: brinda a las instancias de su entorno de trabajo acceso para que carguen archivos de registro en Amazon S3, utilicen Amazon SQS para supervisar la cola de trabajos de su solicitud, para que utilicen Amazon DynamoDB para elegir líderes y Amazon CloudWatch para publicar métricas para la supervisión del estado.

Uso de la política

Puede asociar `AWSElasticBeanstalkWorkerTier` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de febrero de 2016 a las 23:12 UTC
- Hora de edición: 9 de septiembre de 2020 a las 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MetricsAccess",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ]
    }
  ]
}
```

```
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "QueueAccess",
    "Action" : [
      "sqs:ChangeMessageVisibility",
      "sqs:DeleteMessage",
      "sqs:ReceiveMessage",
      "sqs:SendMessage"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "BucketAccess",
    "Action" : [
      "s3:Get*",
      "s3:List*",
      "s3:PutObject"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:s3:::elasticbeanstalk-*",
      "arn:aws:s3:::elasticbeanstalk-*/*"
    ]
  },
  {
    "Sid" : "DynamoPeriodicTasks",
    "Action" : [
      "dynamodb:BatchGetItem",
      "dynamodb:BatchWriteItem",
      "dynamodb:DeleteItem",
      "dynamodb:GetItem",
      "dynamodb:PutItem",
      "dynamodb:Query",
      "dynamodb:Scan",
      "dynamodb:UpdateItem"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
    ]
  }
]
```

```
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryAgentInstallationPolicy

AWSElasticDisasterRecoveryAgentInstallationPolicy es una [política administrada por AWS](#) que: permite instalar el Agente de replicación de AWS, que se usa con la Recuperación de desastres Elastic (DRS) de AWS para recuperar servidores externos en AWS. Asocie esta política a

los usuarios o roles de IAM cuyas credenciales proporciona en el paso de instalación del Agente de replicación de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryAgentInstallationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de noviembre de 2021 a las 10:37 UTC
- Hora editada: 27 de noviembre de 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSAgentInstallationPolicy2",
    "Effect" : "Allow",
    "Action" : "drs:TagResource",
    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
      "StringEquals" : {
        "drs:CreateAction" : "CreateSourceServerForDrs"
      }
    }
  },
  {
    "Sid" : "DRSAgentInstallationPolicy3",
    "Effect" : "Allow",
    "Action" : "drs:TagResource",
    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
      "StringEquals" : {
        "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
      }
    }
  },
  {
    "Sid" : "DRSAgentInstallationPolicy4",
    "Effect" : "Allow",
    "Action" : "drs:TagResource",
    "Resource" : "arn:aws:drs:*:*:source-network/*",
    "Condition" : {
      "StringEquals" : {
        "drs:CreateAction" : "CreateSourceNetwork"
      }
    }
  },
  {
    "Sid" : "DRSAgentInstallationPolicy5",
    "Effect" : "Allow",
    "Action" : "drs:IssueAgentCertificateForDrs",
    "Resource" : "arn:aws:drs:*:*:source-server/*"
  }
]
```

```
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryAgentPolicy

AWSElasticDisasterRecoveryAgentPolicy es una [política administrada por AWS](#) que: permite usar el Agente de replicación de AWS, que se usa con la Recuperación de desastres Elastic (DRS) de AWS para recuperar los servidores de origen de AWS. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryAgentPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 10:32 UTC
- Hora editada: 27 de noviembre de 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
    },
    {
      "Sid" : "DRSAgentPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryConsoleFullAccess

AWSElasticDisasterRecoveryConsoleFullAccess es una [política administrada por AWS](#) que: brinda acceso completo a todas las API públicas de la Recuperación de desastres Elastic (DRS) de AWS, así como permisos para leer la clave de KMS, License Manager, Resource Groups, Elastic Load Balancing, IAM y la información de EC2. Asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de noviembre de 2021 a las 10:46 UTC
- Hora de edición: 16 de octubre de 2023 a las 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
{
  "Sid" : "ConsoleFullAccess1",
  "Effect" : "Allow",
  "Action" : [
    "drs:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess2",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeCapacityReservations",
    "ec2:DescribeHosts"
  ],
  "Resource" : "*"
},
{
```

```

    "Sid" : "ConsoleFullAccess4",
    "Effect" : "Allow",
    "Action" : "license-manager:ListLicenseConfigurations",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess5",
    "Effect" : "Allow",
    "Action" : "resource-groups:ListGroups",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess6",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess7",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess8",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryRecoveryInstanceRole"
    ],
    "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" : "*"
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

AWSElasticDisasterRecoveryConsoleFullAccess_v2 es una [política AWS administrada](#) que: esta política proporciona acceso completo a todas las API públicas de AWS Elastic Disaster Recovery (AWSDRS), así como a todas las API públicas de otros AWS servicios utilizados por AWS DRS Console. Adjunte esta política a sus usuarios o funciones.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryConsoleFullAccess_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2023 a las 13:35 UTC
- Hora editada: 27 de noviembre de 2023 a las 13:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstanceTypeOfferings",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribeLaunchTemplates",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSubnets",
      "ec2:DescribeVolumes",
      "ec2:GetEbsEncryptionByDefault",
      "ec2:GetEbsDefaultKmsKeyId",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeCapacityReservations",
      "ec2:DescribeHosts"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess4",
    "Effect" : "Allow",
    "Action" : "license-manager:ListLicenseConfigurations",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess5",
    "Effect" : "Allow",
    "Action" : "resource-groups: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",
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2::*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  }

```

```
    }
  },
  {
    "Sid" : "ConsoleFullAccess10",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2>DeleteLaunchTemplateVersions",
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess11",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess12",
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
```



```
        "aws:ViaAWSService" : "true"
    }
}
},
{
  "Sid" : "ConsoleFullAccess13",
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess14",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
```

```
"Sid" : "ConsoleFullAccess15",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateVolume"
],
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
}
},
{
  "Sid" : "ConsoleFullAccess16",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSecurityGroup",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "ConsoleFullAccess17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}
},
{
  "Sid" : "ConsoleFullAccess18",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
"Condition" : {
  "Null" : {
    "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
},
{
  "Sid" : "ConsoleFullAccess19",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess20",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess21",
```

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume",
      "ec2:AttachVolume",
      "ec2:StartInstances",
      "ec2:GetConsoleOutput",
      "ec2:GetConsoleScreenshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "drs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess22",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess23",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {

```

```
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  },
  {
    "Sid" : "ConsoleFullAccess24",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess25",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:launch-template*"
    ],
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess26",
    "Effect" : "Allow",
```

```

    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateSecurityGroup",
          "CreateVolume",
          "CreateSnapshot",
          "RunInstances"
        ]
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess27",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateLaunchTemplate"
        ]
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess28",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStacks",
      "cloudformation:ListStacks"
    ],
    "Resource" : "*"
  },
  {

```

```

    "Sid" : "ConsoleFullAccess29",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess30",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeInstanceInformation"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "drs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess31",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand",
      "ssm:StartAutomationExecution"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
      "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
      "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
      "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
      "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
    ],
    "Condition" : {

```

```
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "ConsoleFullAccess32",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "drs.amazonaws.com"
        ]
      },
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess33",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListDocuments",
      "ssm:ListCommandInvocations"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess34",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameter",
      "ssm:PutParameter"
    ],
  },
```



```
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecoveryService-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess35",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:GetDocument"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/*"
  },
  {
    "Sid" : "ConsoleFullAccess36",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameters"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess37",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  }
}
```

```
}  
  ]  
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryConversionServerPolicy

AWSElasticDisasterRecoveryConversionServerPolicy es una [política administrada por AWS](#) que: está asociada al rol de instancia del servidor de la Recuperación de desastres de Elastic de AWS. Esta política permite que los Servidores de conversión de la Recuperación de desastres Elastic (DRS), que son instancias EC2 lanzadas por la Recuperación de desastres Elastic, se comuniquen con el servicio DRS. Con esta política, DRS asocia un rol de IAM (como perfil de instancia EC2) a los Servidores de conversión de DRS, que DRS lanza y termina automáticamente cuando es necesario. No es recomendable que asocie esta política a sus usuarios o roles de IAM. La Recuperación de desastres Elastic utiliza los Servidores de conversión DRS cuando los usuarios eligen recuperar los servidores de origen mediante la consola, la CLI o la API de DRS.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryConversionServerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 13:42 UTC
- Hora editada: 27 de noviembre de 2023, 13:13 UTC

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

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSConversionServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSConversionServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy es una [política administrada por AWS](#) que: permite que la Recuperación de desastres Elastic (DRS) de AWS admita la replicación entre cuentas y la conmutación por recuperación entre cuentas.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryCrossAccountReplicationPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de mayo de 2023 a las 07:16 UTC
- Hora editada: 17 de enero de 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CrossAccountPolicy1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVolumes",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeInstances",
      "drs:DescribeSourceServers",
      "drs:DescribeReplicationConfigurationTemplates",
      "drs:CreateSourceServerForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CrossAccountPolicy2",
    "Effect" : "Allow",
    "Action" : [
      "drs:TagResource"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
      "StringEquals" : {
        "drs:CreateAction" : "CreateSourceServerForDrs"
      }
    }
  }
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryEc2InstancePolicy

AWSElasticDisasterRecoveryEc2InstancePolicy es una [política administrada por AWS](#) que: permite instalar y usar el Agente de replicación de AWS, que usa la recuperación de desastres Elastic (DRS) de AWS para recuperar los servidores de origen que se ejecutan en EC2 (entre regiones o entre zonas de disponibilidad). Con esta política, se debe asociar un rol de IAM (como un perfil de instancia de EC2) a las instancias de EC2.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryEc2InstancePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de mayo de 2022 a las 12:30 UTC
- Hora editada: 27 de noviembre de 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
```

```
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
    ],
    "Resource" : "*"
},
{
    "Sid" : "DRSEc2InstancePolicy2",
    "Effect" : "Allow",
    "Action" : [
        "drs:TagResource"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
        "StringEquals" : {
            "drs:CreateAction" : "CreateSourceServerForDrs"
        }
    }
},
{
    "Sid" : "DRSEc2InstancePolicy3",
    "Effect" : "Allow",
    "Action" : [
        "drs:TagResource"
    ],
    "Resource" : "arn:aws:drs:*:*:source-network/*",
    "Condition" : {
        "StringEquals" : {
            "drs:CreateAction" : "CreateSourceNetwork"
        }
    }
},
{
    "Sid" : "DRSEc2InstancePolicy4",
    "Effect" : "Allow",
    "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
```

```

    "drs:GetAgentRuntimeConfigurationForDrs",
    "drs:UpdateAgentBacklogForDrs",
    "drs:GetAgentReplicationInfoForDrs"
  ],
  "Resource" : "arn:aws:drs:*:*:source-server/*"
},
{
  "Sid" : "DRSEc2InstancePolicy5",
  "Effect" : "Allow",
  "Action" : [
    "sts:AssumeRole",
    "sts:TagSession"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
    },
    "ForAnyValue:StringEquals" : {
      "sts:TransitiveTagKeys" : "SourceInstanceARN"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

AWSElasticDisasterRecoveryFailbackInstallationPolicy es una [política AWS gestionada](#) que: puede adjuntar la AWSElasticDisasterRecoveryFailbackInstallationPolicy política a sus identidades de IAM. Esta política permite instalar el cliente de conmutación por recuperación de la Recuperación de desastres Elastic, que se utiliza para devolver las instancias de recuperación a la infraestructura de origen original. Asocie esta política a los usuarios o roles de IAM cuyas credenciales proporciona al ejecutar el cliente de conmutación por recuperación de la Recuperación de desastres Elastic.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryFailbackInstallationPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de noviembre de 2021 a las 11:02 UTC
- Hora editada: 27 de noviembre de 2023 a las 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

{
  "Sid" : "DRSFailbackInstallationPolicy1",
  "Effect" : "Allow",
  "Action" : [
    "drs:SendClientLogsForDrs",
    "drs:SendClientMetricsForDrs",
    "drs:DescribeRecoveryInstances",
    "drs:DescribeSourceServers"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSFailbackInstallationPolicy2",
  "Effect" : "Allow",
  "Action" : [
    "drs:TagResource",
    "drs:IssueAgentCertificateForDrs",
    "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
    "drs:GetSuggestedFailbackClientDeviceMappingForDrs",
    "drs:UpdateAgentReplicationInfoForDrs",
    "drs:UpdateFailbackClientDeviceMappingForDrs"
  ],
  "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryFailbackPolicy

AWSElasticDisasterRecoveryFailbackPolicy es una [política administrada por AWS](#) que: permite utilizar el Cliente de conmutación por recuperación de la Recuperación de desastres, que

se usa para devolver las instancias de recuperación a la infraestructura de origen original. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryFailbackPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 10:41 UTC
- Hora editada: 27 de noviembre de 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
```

```

    "Effect" : "Allow",
    "Action" : [
      "drs:GetChannelCommandsForDrs",
      "drs:SendChannelCommandResultForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSFailbackPolicy3",
    "Effect" : "Allow",
    "Action" : [
      "drs:DescribeReplicationServerAssociationsForDrs",
      "drs:DescribeRecoveryInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSFailbackPolicy4",
    "Effect" : "Allow",
    "Action" : [
      "drs:GetFailbackCommandForDrs",
      "drs:UpdateFailbackClientLastSeenForDrs",
      "drs:NotifyAgentAuthenticationForDrs",
      "drs:UpdateAgentReplicationProcessStateForDrs",
      "drs:NotifyAgentReplicationProgressForDrs",
      "drs:NotifyAgentConnectedForDrs",
      "drs:NotifyAgentDisconnectedForDrs",
      "drs:NotifyConsistencyAttainedForDrs",
      "drs:GetFailbackLaunchRequestedForDrs",
      "drs:IssueAgentCertificateForDrs"
    ],
    "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

AWSElasticDisasterRecoveryLaunchActionsPolicy es una [política administrada por AWS](#) que: le permite utilizar Amazon SSM y los permisos necesarios para ejecutar acciones posteriores al lanzamiento en la recuperación de desastres Elastic de AWS (DRS de AWS). Asocie esta política a sus roles o usuarios de IAM.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryLaunchActionsPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de septiembre de 2023 a las 07:38 UTC
- Hora de edición: 16 de octubre de 2023 a las 12:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

AWSElasticDisasterRecoveryNetworkReplicationPolicy es una [política administrada por AWS](#) que: permite que la Recuperación de desastres Elastic (DRS) de AWS admita la replicación de la red.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryNetworkReplicationPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de junio de 2023 a las 12:36 UTC
- Hora editada: 2 de enero de 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
```

```
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeRouteTables",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeInstances",
    "ec2:DescribeManagedPrefixLists",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetManagedPrefixListAssociations"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryReadOnlyAccess

AWSElasticDisasterRecoveryReadOnlyAccesses una [política AWS gestionada](#) que: puede adjuntar la AWSElasticDisasterRecoveryReadOnlyAccess política a sus identidades de IAM. Esta política otorga permisos de solo lectura a todas las API públicas de la Recuperación de desastres Elastic (DRS). También, concede permisos de solo lectura a algunas API de otros servicios de AWS que se requieren para poder utilizar completamente la consola de DRS en modo de solo lectura. Asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de noviembre de 2021 a las 10:50 UTC
- Hora editada: 27 de noviembre de 2023 a las 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
  ],
}
```

```

{
  "Sid" : "DRSReadOnlyAccess2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets"
  ],
  "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"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

AWSElasticDisasterRecoveryRecoveryInstancePolicy es una [política administrada por AWS](#) que: está asociada al rol de instancia de la instancia de Recuperación de desastres Elastic. Esta política permite que las instancias de recuperación de la Recuperación de desastres Elastic (DRS), que son instancias EC2 lanzadas por Recuperación de desastres Elastic, se comuniquen con el servicio DRS y puedan realizar una conmutación a su infraestructura de origen original. Con esta política, la Recuperación de desastres Elastic asocia un rol de IAM (como perfil de instancia EC2) a las instancias de recuperación de DRS. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryRecoveryInstancePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 10:20 UTC
- Hora editada: 27 de noviembre de 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
      ]
    }
  ]
}
```

```

    "drs:UpdateReplicationCertificateForDrs",
    "drs:NotifyReplicationServerAuthenticationForDrs"
  ],
  "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
  "Condition" : {
    "StringEquals" : {
      "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
    }
  }
},
{
  "Sid" : "DRSRecoveryInstancePolicy2",
  "Effect" : "Allow",
  "Action" : [
    "drs:DescribeRecoveryInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSRecoveryInstancePolicy3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstanceTypes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSRecoveryInstancePolicy4",
  "Effect" : "Allow",
  "Action" : [
    "drs:GetAgentInstallationAssetsForDrs",
    "drs:SendClientLogsForDrs",
    "drs:CreateSourceServerForDrs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSRecoveryInstancePolicy5",
  "Effect" : "Allow",
  "Action" : [
    "drs:TagResource"
  ],
  "Resource" : "arn:aws:drs:*:*:source-server/*",
  "Condition" : {

```

```

    "StringEquals" : {
      "drs:CreateAction" : "CreateSourceServerForDrs"
    }
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy6",
    "Effect" : "Allow",
    "Action" : [
      "drs:SendAgentMetricsForDrs",
      "drs:SendAgentLogsForDrs",
      "drs:UpdateAgentSourcePropertiesForDrs",
      "drs:UpdateAgentReplicationInfoForDrs",
      "drs:UpdateAgentConversionInfoForDrs",
      "drs:GetAgentCommandForDrs",
      "drs:GetAgentConfirmedResumeInfoForDrs",
      "drs:GetAgentRuntimeConfigurationForDrs",
      "drs:UpdateAgentBacklogForDrs",
      "drs:GetAgentReplicationInfoForDrs"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*"
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy7",
    "Effect" : "Allow",
    "Action" : [
      "sts:AssumeRole",
      "sts:TagSession"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
      },
      "ForAnyValue:StringEquals" : {
        "sts:TransitiveTagKeys" : "SourceInstanceARN"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

AWSElasticDisasterRecoveryReplicationServerPolicy es una [política administrada por AWS](#) que: está asociada al rol de instancia del servidor de replicación de la Recuperación de desastres Elastic. Esta política permite que los Servidores de replicación de la Recuperación de desastres Elastic (DRS), que son instancias EC2 lanzadas por la Recuperación de desastres Elastic, se comuniquen con el servicio DRS y creen capturas de EBS en sus servidores de Cuenta de AWS. Con esta política, la Recuperación de desastres Elastic asigna un rol de IAM (como perfil de instancia EC2) a los Servidores de replicación de DRS, que DRS lanza y termina automáticamente, según sea necesario. Los Servidores de replicación DRS se utilizan para facilitar la replicación de datos desde sus servidores externos de AWS, como parte del proceso de recuperación gestionado por DRS. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar AWSElasticDisasterRecoveryReplicationServerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 13:34 UTC
- Hora editada: 27 de noviembre de 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReplicationServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeSnapshotRequestsForDrs",
        "drs:BatchDeleteSnapshotRequestForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:BatchCreateVolumeSnapshotGroupForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
```

```
    "drs:NotifyAgentConnectedForDrs",
    "drs:NotifyAgentDisconnectedForDrs",
    "drs:NotifyVolumeEventForDrs",
    "drs:SendVolumeStatsForDrs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSReplicationServerPolicy4",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSReplicationServerPolicy5",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSReplicationServerPolicy6",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSReplicationServerPolicy7",
```

```
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSnapshot"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryServiceRolePolicy

AWSElasticDisasterRecoveryServiceRolePolicy es una [política administrada por AWS](#) que: permite que la Recuperación de desastres Elastic administre los recursos de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2021 a las 10:56 UTC
- Hora editada: 17 de enero de 2024, 13:49 UTC

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

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
```



```
"Sid" : "DRSServiceRolePolicy4",
"Effect" : "Allow",
"Action" : "iam:GetInstanceProfile",
"Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy5",
  "Effect" : "Allow",
  "Action" : "kms:ListRetirableGrants",
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy6",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVolumeAttribute",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeVpcs",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeManagedPrefixLists",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetManagedPrefixListAssociations"
  ],
  "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" : "*"
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

AWSElasticDisasterRecoveryStagingAccountPolicy es una [política administrada por AWS](#) que: permite el acceso de solo lectura a los recursos de la Recuperación de desastres Elastic

(DRS) de AWS, como los servidores de origen y los trabajos. También, permite crear una captura convertida y compartirla con una cuenta específica.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryStagingAccountPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de mayo de 2022 a las 09:49 UTC
- Hora editada: 27 de noviembre de 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
```

```

    "drs:DescribeJobLogItems"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSStagingAccountPolicy2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:Add/userId" : "${aws:SourceIdentity}"
    },
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 es una [política administrada por AWS](#) que: la recuperación de desastres Elastic (DRS) de AWS utiliza para recuperar los servidores de origen en una cuenta de destino independiente y para permitir la recuperación de errores. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de enero de 2023 a las 12:11 UTC
- Hora editada: 27 de noviembre de 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
  ],
}
```

```

    "Sid" : "DRSStagingAccountPolicyv22",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifySnapshotAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:Add/userId" : "${aws:SourceIdentity}"
      },
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSStagingAccountPolicyv23",
    "Effect" : "Allow",
    "Action" : "drs:IssueAgentCertificateForDrs",
    "Resource" : [
      "arn:aws:drs:*:*:source-server/*"
    ]
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

AWSElasticLoadBalancingClassicServiceRolePolicy es una [política administrada por AWS](#) que: es una Política de roles vinculados a un servicio para el plano de control de AWS Elastic Load Balancing: Clásico

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de septiembre de 2017 a las 22:36 UTC
- Hora de edición: 7 de octubre de 2019 a las 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",

```

```
    "ec2:CreateSecurityGroup",
    "ec2:CreateNetworkInterface",
    "ec2>DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:AttachNetworkInterface",
    "ec2:DetachNetworkInterface",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssignIpv6Addresses",
    "ec2:UnassignIpv6Addresses"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElasticLoadBalancingServiceRolePolicy

AWSElasticLoadBalancingServiceRolePolicy es una [política administrada por AWS](#) que: es una Política de roles vinculados a un servicio para el plano de control de AWS Elastic Load Balancing: Clásico

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de septiembre de 2017 a las 22:19 UTC

- Hora de edición: 26 de agosto de 2021 a las 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2: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" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaConvertFullAccess

AWSElementalMediaConvertFullAccess es una [política administrada por AWS](#) que: brinda acceso completo a AWS Elemental MediaConvert a través de la AWS Management Console y SDK.

Uso de la política

Puede asociar AWSElementalMediaConvertFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de junio de 2018 a las 19:25 UTC
- Hora de edición: 10 de junio de 2019 a las 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "mediaconvert.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaConvertReadOnly

AWSElementalMediaConvertReadOnly es una [política administrada por AWS](#) que: concede acceso de solo lectura a AWS Elemental MediaConvert de a través de la AWS Management Console y SDK.

Uso de la política

Puede asociar AWSElementalMediaConvertReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de junio de 2018 a las 19:25 UTC
- Hora de edición: 10 de junio de 2019 a las 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "mediaconvert:Get*",
      "mediaconvert:List*",
      "mediaconvert:DescribeEndpoints",
      "s3:ListAllMyBuckets",
      "s3:ListBucket"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaLiveFullAccess

AWSElementalMediaLiveFullAccess es una [política administrada por AWS](#) que: brinda acceso completo a los recursos de AWS Elemental MediaLive

Uso de la política

Puede asociar AWSElementalMediaLiveFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de julio de 2020 a las 17:07 UTC
- Hora de edición: 8 de julio de 2020 a las 17:07 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaLiveReadOnly

AWSElementalMediaLiveReadOnly es una [política administrada por AWS](#) que: concede acceso de solo lectura a los recursos de AWS Elemental MediaLive

Uso de la política

Puede asociar AWSElementalMediaLiveReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de julio de 2020 a las 16:38 UTC
- Hora de edición: 8 de julio de 2020 a las 16:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaPackageFullAccess

AWSElementalMediaPackageFullAccess es una [política administrada por AWS](#) que: brinda acceso total a los recursos de Elemental MediaPackage de AWS

Uso de la política

Puede asociar AWSElementalMediaPackageFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de diciembre de 2017 a las 23:39 UTC
- Hora de edición: 29 de diciembre de 2017 a las 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaPackageReadOnly

AWSElementalMediaPackageReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura a los recursos de Elemental MediaPackage de AWS

Uso de la política

Puede asociar AWSElementalMediaPackageReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de diciembre de 2017 a las 00:04 UTC
- Hora de edición: 30 de diciembre de 2017 a las 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "mediapackage:List*",
    "mediapackage:Describe*"
  ],
  "Resource" : "*"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaPackageV2FullAccess

AWSElementalMediaPackageV2FullAccess es una [política administrada por AWS](#) que: otorga acceso total a los recursos de Elemental MediaPackageV2 de AWS.

Uso de la política

Puede asociar AWSElementalMediaPackageV2FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de julio de 2023 a las 20:29 UTC
- Hora de edición: 25 de julio de 2023 a las 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaPackageV2ReadOnly

AWSElementalMediaPackageV2ReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura a los recursos de Elemental MediaPackageV2 de AWS.

Uso de la política

Puede asociar AWSElementalMediaPackageV2ReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de julio de 2023 a las 20:31 UTC
- Hora de edición: 25 de julio de 2023 a las 20:31 UTC

- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaStoreFullAccess

`AWSElementalMediaStoreFullAccess` es una [política administrada por AWS](#) que: proporciona acceso total de lectura y escritura a todas las API de MediaStore

Uso de la política

Puede asociar `AWSElementalMediaStoreFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de marzo de 2018 a las 23:15 UTC
- Hora de edición: 5 de marzo de 2018 a las 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaStoreReadOnly

AWSElementalMediaStoreReadOnly es una [política administrada AWS](#) que: otorga permisos de solo lectura para las API de MediaStore

Uso de la política

Puede asociar AWSElementalMediaStoreReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de marzo de 2018 a las 19:48 UTC
- Hora de edición: 8 de marzo de 2018 a las 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Action" : [
      "mediastore:Get*",
      "mediastore:List*",
      "mediastore:Describe*"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "aws:SecureTransport" : "true"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaTailorFullAccess

AWSElementalMediaTailorFullAccess es una [política administrada por AWS](#) que: brinda acceso total a los recursos de Elemental MediaTailor de AWS

Uso de la política

Puede asociar AWSElementalMediaTailorFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 23 de noviembre de 2021 a las 00:04 UTC
- Hora de edición: 23 de noviembre de 2021 a las 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSElementalMediaTailorReadOnly

AWSElementalMediaTailorReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura a los recursos de Elemental MediaTailor de AWS

Uso de la política

Puede asociar `AWSElementalMediaTailorReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de noviembre de 2021 a las 00:05 UTC
- Hora de edición: 23 de noviembre de 2021 a las 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSEnhancedClassicNetworkingMangementPolicy

AWSEnhancedClassicNetworkingMangementPolicy es una [política administrada por AWS](#) que: habilita la característica de administración de redes clásica mejorada.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de septiembre de 2017 a las 17:29 UTC
- Hora de edición: 20 de septiembre de 2017 a las 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Statement" : [
  {
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSEntityResolutionConsoleFullAccess

AWSEntityResolutionConsoleFullAccess es una [política administrada por AWS](#) que: proporciona a la consola acceso total a AWS Entity Resolution y a los servicios relacionados.

Uso de la política

Puede asociar AWSEntityResolutionConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de agosto de 2023 a las 17:54 UTC
- Hora de edición: 16 de octubre de 2023 a las 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketsConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Sid" : "S3SourcesConsoleDisplay",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:ListBucketVersions",
    "s3:GetBucketVersioning"
  ],
  "Resource" : "*"
},
{
  "Sid" : "TaggingConsoleDisplay",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetTagKeys",
    "tag:GetTagValues"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KMSConsoleDisplay",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ListRolesToPickRoleForPassing",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PassRoleToEntityResolutionService",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*entityresolution*",
}
```

```
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "entityresolution.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ManageEventBridgeRules",
    "Effect" : "Allow",
    "Action" : [
      "events:DeleteRule",
      "events:PutTargets",
      "events:PutRule"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/entity-resolution-automatic*"
    ]
  },
  {
    "Sid" : "ADXReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "dataexchange:GetDataSet"
    ],
    "Resource" : "*"
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSEntityResolutionConsoleReadOnlyAccess

AWSEntityResolutionConsoleReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a AWS Entity Resolution a través de la AWS Management Console.

Uso de la política

Puede asociar AWSEntityResolutionConsoleReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de agosto de 2023 a las 18:18 UTC
- Hora de edición: 17 de agosto de 2023 a las 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFaultInjectionSimulatorEC2Access

AWSFaultInjectionSimulatorEC2Access es una [política administrada por AWS](#) que: concede al servicio de simulador de inyección de fallos el permiso en EC2 y otros servicios que se necesitan para realizar acciones de FIS.

Uso de la política

Puede asociar AWSFaultInjectionSimulatorEC2Access a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:39 UTC
- Hora editada: 27 de noviembre de 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    }
  ],
  {
    "Sid" : "AllowSSMSendOnEc2",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
```

```
    "arn:aws:ssm:*:*:document/*"
  ],
},
{
  "Sid" : "AllowSSMStopOnEc2",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CancelCommand",
    "ssm:ListCommands"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DescribeInstances",
  "Effect" : "Allow",
  "Action" : "ec2:DescribeInstances",
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFaultInjectionSimulatorECSAccess

AWSFaultInjectionSimulatorECSAccess es una [política administrada por AWS](#) que: otorga al servicio de simulador de inyección de fallas permiso en el ECS y otros servicios que se necesitan para realizar acciones de FIS.

Uso de la política

Puede asociar AWSFaultInjectionSimulatorECSAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:37 UTC
- Hora editada: 25 de enero de 2024, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
```

```
    "arn:aws:ecs:*:*:task/*/*"
  ]
},
{
  "Sid" : "ContainerInstances",
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateContainerInstancesState"
  ],
  "Resource" : [
    "arn:aws:ecs:*:*:container-instance/*/*"
  ]
},
{
  "Sid" : "ListTasks",
  "Effect" : "Allow",
  "Action" : [
    "ecs:ListTasks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SSMSend",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ssm:*:*:managed-instance/*",
    "arn:aws:ssm:*:*:document/*"
  ]
},
{
  "Sid" : "SSMList",
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListCommands",
    "ssm:CancelCommand"
  ],
  "Resource" : "*"
},
{
  "Sid" : "TargetResolutionByTags",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
```

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFaultInjectionSimulatorEKSAccess

AWSFaultInjectionSimulatorEKSAccess es una [política administrada por AWS](#) que: otorga al servicio de simulador de inyección de fallas permiso en el EKS y otros servicios que se necesitan para realizar acciones de FIS.

Uso de la política

Puede asociar AWSFaultInjectionSimulatorEKSAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:34 UTC
- Hora de edición: 13 de noviembre de 2023 a las 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DescribeNodeGroup",
      "Effect" : "Allow",
      "Action" : "eks:DescribeNodegroup",
      "Resource" : "arn:aws:eks:*:*:nodegroup/*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
```

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFaultInjectionSimulatorNetworkAccess

AWSFaultInjectionSimulatorNetworkAccess es una [política administrada por AWS](#) que: concede al servicio de simulador de inyección de fallos permiso en las redes de EC2 y otros servicios que se necesitan para realizar acciones de FIS.

Uso de la política

Puede asociar AWSFaultInjectionSimulatorNetworkAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:32 UTC
- Hora editada: 25 de enero de 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkAcl",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2>DeleteNetworkAcl"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
    }
  ],
}
```

```

    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateNetworkAclOnVpc",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkAcl",
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid" : "VpcActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs",
      "ec2:DescribeManagedPrefixLists",
      "ec2:DescribeSubnets",
      "ec2:DescribeNetworkAcls",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeVpcPeeringConnections",
      "ec2:DescribeRouteTables",
      "ec2:DescribeTransitGatewayPeeringAttachments",
      "ec2:DescribeTransitGatewayAttachments",
      "ec2:DescribeTransitGateways"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ReplaceNetworkAclAssociation",
    "Effect" : "Allow",
    "Action" : "ec2:ReplaceNetworkAclAssociation",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:network-acl/*"
    ]
  },
  {
    "Sid" : "GetManagedPrefixListEntries",
    "Effect" : "Allow",
    "Action" : "ec2:GetManagedPrefixListEntries",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
  }
}

```

```
  },
  {
    "Sid" : "CreateRouteTable",
    "Effect" : "Allow",
    "Action" : "ec2:CreateRouteTable",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateRouteTableOnVpc",
    "Effect" : "Allow",
    "Action" : "ec2:CreateRouteTable",
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid" : "CreateTagsOnRouteTable",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateRouteTable",
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateTagsOnNetworkInterface",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface",
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateTagsOnPrefixList",
```



```

    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateManagedPrefixList",
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "DeleteRouteTable",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteRouteTable",
    "Resource" : [
      "arn:aws:ec2:*:*:route-table/*",
      "arn:aws:ec2:*:*:vpc/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateRoute",
    "Effect" : "Allow",
    "Action" : "ec2:CreateRoute",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateNetworkInterface",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  }
}

```

```

    }
  },
  {
    "Sid" : "CreateNetworkInterfaceOnSubnet",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Sid" : "DeleteNetworkInterface",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateManagedPrefixList",
    "Effect" : "Allow",
    "Action" : "ec2:CreateManagedPrefixList",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "DeleteManagedPrefixList",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteManagedPrefixList",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  }
},

```

```

{
  "Sid" : "ModifyManagedPrefixList",
  "Effect" : "Allow",
  "Action" : "ec2:ModifyManagedPrefixList",
  "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "ReplaceRouteTableAssociation",
  "Effect" : "Allow",
  "Action" : "ec2:ReplaceRouteTableAssociation",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "AssociateRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:AssociateRouteTable",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "DisassociateRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:DisassociateRouteTable",
  "Resource" : [
    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "DisassociateRouteTableOnSubnet",

```

```
    "Effect" : "Allow",
    "Action" : "ec2:DisassociateRouteTable",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*"
    ]
  },
  {
    "Sid" : "ModifyVpcEndpointOnRouteTable",
    "Effect" : "Allow",
    "Action" : "ec2:ModifyVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:route-table/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "ModifyVpcEndpoint",
    "Effect" : "Allow",
    "Action" : "ec2:ModifyVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:vpc-endpoint/*"
    ]
  },
  {
    "Sid" : "TransitGatewayRouteTableAssociation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DisassociateTransitGatewayRouteTable",
      "ec2:AssociateTransitGatewayRouteTable"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:transit-gateway-route-table/*",
      "arn:aws:ec2:*:*:transit-gateway-attachment/*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFaultInjectionSimulatorRDSAccess

AWSFaultInjectionSimulatorRDSAccess es una [política administrada por AWS](#) que: concede al servicio de simulador de inyección de fallos permiso en RDS y otros servicios necesarios para realizar acciones de FIS.

Uso de la política

Puede asociar AWSFaultInjectionSimulatorRDSAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:30 UTC
- Hora de edición: 13 de noviembre de 2023 a las 16:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
      "Effect" : "Allow",
      "Action" : [
        "rds:RebootDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

}

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFaultInjectionSimulatorSSMAccess

AWSFaultInjectionSimulatorSSMAccess es una [política administrada por AWS](#) que: concede al servicio de simulador de inyección de fallos permiso en SSM y otros servicios necesarios para realizar acciones de FIS.

Uso de la política

Puede asociar AWSFaultInjectionSimulatorSSMAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 15:33 UTC
- Hora de edición: 2 de junio de 2023, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm::*: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" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFinSpaceServiceRolePolicy

AWSFinSpaceServiceRolePolicy es una [política AWS gestionada](#) que: Política para permitir el acceso Servicio de AWS y los recursos utilizados o gestionados por Amazon FinSpace

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de mayo de 2023 a las 16:42 UTC
- Hora editada: 1 de diciembre de 2023 a las 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFMAdminFullAccess

AWSFMAdminFullAccess es una [política administrada por AWS](#) que: otorga acceso total para el administrador de FM de AWS

Uso de la política

Puede asociar `AWSFMAdminFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de mayo de 2018 a las 18:06 UTC
- Hora de edición: 20 de octubre de 2022 a las 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
```

```

    "route53resolver:ListFirewallRuleGroups",
    "route53resolver:GetFirewallRuleGroup",
    "wafv2:ListRuleGroups",
    "wafv2:ListAvailableManagedRuleGroups",
    "wafv2:CheckCapacity",
    "wafv2:PutLoggingConfiguration",
    "wafv2:ListAvailableManagedRuleGroupVersions",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:DescribeRuleGroupMetadata",
    "network-firewall:ListRuleGroups",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeRegions"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketPolicy",
    "s3:GetBucketPolicy"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-waf-logs-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "fms.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ]
}

```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "fms.amazonaws.com"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFMAdminReadOnlyAccess

AWSFMAdminReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura para el administrador de FM a AWS que permite monitorear las operaciones de FM de AWS

Uso de la política

Puede asociar AWSFMAdminReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de mayo de 2018 a las 20:07 UTC
- Hora de edición: 31 de octubre de 2022 a las 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:Get*",
        "fms:List*",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketPolicy"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-waf-logs-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "fms.amazonaws.com"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSFMMemberReadOnlyAccess

`AWSFMMemberReadOnlyAccess` es una [política administrada por AWS](#) que: brinda acceso de solo lectura a las acciones de AWS WAF para las cuentas de los miembros de AWS Firewall Manager

Uso de la política

Puede asociar `AWSFMMemberReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de mayo de 2018 a las 21:05 UTC
- Hora de edición: 9 de mayo de 2018 a las 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
    }
  ]
}
```



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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSForWordPressPluginPolicy

AWSForWordPressPluginPolicy es una [política administrada por AWS](#) para: el complemento AWS For Wordpress

Uso de la política

Puede asociar AWSForWordPressPluginPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de octubre de 2019 a las 00:27 UTC
- Hora de edición: 20 de enero de 2020 a las 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3>DeleteObject",
        "s3:CreateBucket",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::audio_for_wordpress*",
        "arn:aws:s3:::audio-for-wordpress*"
      ]
    },
    {
      "Sid" : "Permissions3",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DescribeCertificate",
        "acm:RequestCertificate",
        "cloudformation:CreateStack",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "aws:RequestedRegion" : "us-east-1"
      }
    }
  },
  {
    "Sid" : "Permissions4",
    "Effect" : "Allow",
    "Action" : [
      "acm:DeleteCertificate",
      "cloudformation:DeleteStack",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResources",
      "cloudformation:UpdateStack",
      "cloudfront:CreateDistribution",
      "cloudfront:CreateInvalidation",
      "cloudfront>DeleteDistribution",
      "cloudfront:GetDistribution",
      "cloudfront:GetInvalidation",
      "cloudfront:TagResource",
      "cloudfront:UpdateDistribution"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGitSyncServiceRolePolicy

AWSGitSyncServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Code Connections sincronice el contenido de su repositorio de git

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de noviembre de 2023 a las 17:05 UTC
- Hora de edición: 16 de noviembre de 2023 a las 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGlobalAcceleratorSLRPolicy

AWSGlobalAcceleratorSLRPolicy es una [política administrada por AWS](#) que: otorga permisos a AWS Global Accelerator para que gestione las Interfaces de red Elastic y los grupos de seguridad de EC2.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de abril de 2019 a las 19:39 UTC
- Hora de edición: 12 de septiembre de 2023 a las 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2>DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
```

```
    "Action" : [
      "ec2:CreateSecurityGroup",
      "ec2:DescribeSecurityGroups"
    ],
    "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/*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGlueConsoleFullAccess

AWSGlueConsoleFullAccess es una [política administrada por AWS](#) que: concede acceso total a AWS Glue a través de la AWS Management Console

Uso de la política

Puede asociar `AWSGlueConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de agosto de 2017 a las 13:37 UTC
- Hora de edición: 14 de julio de 2023 a las 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAppPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```



```

    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeInstances",
    "ec2:DescribeImages",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "rds:DescribeDBSubnetGroups",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "cloudformation:ListStacks",
    "cloudformation:DescribeStacks",
    "cloudformation:GetTemplateSummary",
    "dynamodb:ListTables",
    "kms:ListAliases",
    "kms:DescribeKey",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListDashboards",
    "databrew:ListRecipes",
    "databrew:ListRecipeVersions",
    "databrew:DescribeRecipe"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*/**",
    "arn:aws:s3:::*/**aws-glue-*/**",
    "arn:aws:s3:::aws-glue-*"
  ]
},
{
  "Effect" : "Allow",

```

```
"Action" : [
  "tag:GetResources"
],
"Resource" : [
  "*"
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:GetLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:/aws-glue/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
```

```

        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2>DeleteTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "StringLike" : {
            "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
            "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
    }
},
{
    "Action" : [
        "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam:*:*:role/AWSGlueServiceRole*",
    "Condition" : {
        "StringLike" : {
            "iam:PassedToService" : [
                "glue.amazonaws.com"
            ]
        }
    }
},
{
    "Action" : [
        "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam:*:*:role/AWSGlueServiceNotebookRole*",

```

```
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    },
  ],
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGlueConsoleSageMakerNotebookFullAccess

AWSGlueConsoleSageMakerNotebookFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS Glue a través de la AWS Management Console y acceso a las instancias de SageMaker Notebook.

Uso de la política

Puede asociar AWSGlueConsoleSageMakerNotebookFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de octubre de 2018 a las 17:52 UTC
- Hora de edición: 15 de julio de 2021 a las 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",

```

```
    "iam:ListAttachedRolePolicies",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeInstances",
    "ec2:DescribeImages",
    "ec2:CreateNetworkInterface",
    "ec2:AttachNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2>DeleteNetworkInterface",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeNetworkInterfaces",
    "rds:DescribeDBInstances",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "cloudformation:DescribeStacks",
    "cloudformation:GetTemplateSummary",
    "dynamodb:ListTables",
    "kms:ListAliases",
    "kms:DescribeKey",
    "sagemaker:ListNotebookInstances",
    "cloudformation:ListStacks",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListDashboards"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*/*aws-glue-*/*",
```

```

    "arn:aws:s3:::aws-glue-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:GetLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:/aws-glue/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreatePresignedNotebookInstanceUrl",
    "sagemaker:CreateNotebookInstance",
    "sagemaker>DeleteNotebookInstance",
    "sagemaker:DescribeNotebookInstance",
    "sagemaker:StartNotebookInstance",
    "sagemaker:StopNotebookInstance",
    "sagemaker:UpdateNotebookInstance",
    "sagemaker:ListTags"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
      "sagemaker:DescribeNotebookInstanceLifecycleConfig",
      "sagemaker>CreateNotebookInstanceLifecycleConfig",
      "sagemaker>DeleteNotebookInstanceLifecycleConfig",
      "sagemaker>ListNotebookInstanceLifecycleConfigs"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:key-pair/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:volume*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2>CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
      },
      "StringEquals" : {
        "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
      }
    }
  }
}

```



```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : [
          "aws-glue-*"
        ]
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  }
}
```

```
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com"
      ]
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AwsGlueDataBrewFullAccessPolicy

AwsGlueDataBrewFullAccessPolicy es una [política administrada por AWS](#) que: concede acceso completo a AWS Glue DataBrew a través de la AWS Management Console. También, proporciona acceso selecto a los servicios relacionados (por ejemplo, S3, KMS, Glue).

Uso de la política

Puede asociar AwsGlueDataBrewFullAccessPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de noviembre de 2020 a las 16:51 UTC
- Hora de edición: 4 de febrero de 2022 a las 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
```

```
"databrew:UpdateDataset",
"databrew:DeleteDataset",
"databrew:CreateProject",
"databrew:DescribeProject",
"databrew:ListProjects",
"databrew:StartProjectSession",
"databrew:SendProjectSessionAction",
"databrew:UpdateProject",
"databrew:DeleteProject",
"databrew:CreateRecipe",
"databrew:DescribeRecipe",
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:PublishRecipe",
"databrew:UpdateRecipe",
"databrew:BatchDeleteRecipeVersion",
"databrew:DeleteRecipeVersion",
"databrew:CreateRecipeJob",
"databrew:CreateProfileJob",
"databrew:DescribeJob",
"databrew:DescribeJobRun",
"databrew:ListJobRuns",
"databrew:ListJobs",
"databrew:StartJobRun",
"databrew:StopJobRun",
"databrew:UpdateProfileJob",
"databrew:UpdateRecipeJob",
"databrew:DeleteJob",
"databrew:CreateSchedule",
"databrew:DescribeSchedule",
"databrew:ListSchedules",
"databrew:UpdateSchedule",
"databrew:DeleteSchedule",
"databrew:CreateRuleset",
"databrew:DeleteRuleset",
"databrew:DescribeRuleset",
"databrew:ListRulesets",
"databrew:UpdateRuleset",
"databrew:ListTagsForResource",
"databrew:TagResource",
"databrew:UntagResource"
],
"Resource" : [
  "*"
]
```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "appflow:DescribeFlow",
    "appflow:DescribeFlowExecutionRecords",
    "appflow:ListFlows",
    "glue:GetConnection",
    "glue:GetConnections",
    "glue:GetDatabases",
    "glue:GetPartitions",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetDataCatalogEncryptionSettings",
    "dataexchange:ListDataSets",
    "dataexchange:ListDataSetRevisions",
    "dataexchange:ListRevisionAssets",
    "dataexchange:CreateJob",
    "dataexchange:StartJob",
    "dataexchange:GetJob",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "kms:DescribeKey",
    "kms:ListKeys",
    "kms:ListAliases",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSubnetGroups",
    "redshift-data:DescribeStatement",
    "redshift-data:ListDatabases",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCORS",
    "s3:GetBucketLocation",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "sts:GetCallerIdentity",
    "cloudtrail:LookupEvents",
    "iam:ListRoles",
    "iam:GetRole"
  ]
}
```

```

    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateConnection"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:GetDatabases"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateTable"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
    ]
}

```

```

    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:GenerateDataKey"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "s3.*.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:GenerateRandom"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "databrew.amazonaws.com"
        ]
      }
    }
  }
},

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
  "Condition" : {
    "StringLike" : {
      "secretsmanager:Name" : "databrew!default"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "databrew.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam:*:*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "databrew.amazonaws.com"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGlueDataBrewServiceRole

AWSGlueDataBrewServiceRole es una [política administrada por AWS](#) que: otorga permiso a Glue para que realice acciones en el catálogo de datos de Glue del usuario. Esta política también otorga permiso a ec2 acciones para permitir que Glue cree ENI para conectarse a los recursos de la VPC. También, permite que Glue acceda a los datos registrados en Lakeformation, y concede permiso para acceder a Cloudwatch del usuario

Uso de la política

Puede asociar AWSGlueDataBrewServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de diciembre de 2020 a las 21:26 UTC
- Hora editada: 20 de marzo de 2024 a las 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```

    "Action" : [
      "glue:GetDatabases",
      "glue:GetPartitions",
      "glue:GetTable",
      "glue:GetTables",
      "glue:GetConnection"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "GluePIIPermissions",
    "Effect" : "Allow",
    "Action" : [
      "glue:BatchGetCustomEntityTypes",
      "glue:GetCustomEntityType"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "S3PublicDatasetAccess",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::databrew-public-datasets-*"
    ]
  },
  {
    "Sid" : "EC2NetworkingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeRouteTables",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcAttribute",
      "ec2:CreateNetworkInterface"
    ]
  }

```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteNetworkInterface",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws-glue-service-resource" : "*"
      }
    },
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "EC2GlueTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2:DeleteTags"
    ],
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "aws-glue-service-resource"
        ]
      }
    },
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group*"
    ]
  },
  {
    "Sid" : "GlueDatabrewLogGroupPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
    ]
  },
  {
    "Sid" : "LakeFormationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "lakeformation:GetDataAccess"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSGlueSchemaRegistryFullAccess

AWSGlueSchemaRegistryFullAccess es una [política administrada por AWS](#) que: brinda acceso completo al servicio de registro de AWS Glue Schema

Uso de la política

Puede asociar `AWSGlueSchemaRegistryFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de noviembre de 2020 a las 00:19 UTC
- Hora de edición: 20 de noviembre de 2020 a las 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
        "glue>DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:CreateSchema",
        "glue:UpdateSchema",
        "glue>DeleteSchema",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:RegisterSchemaVersion",
```

```

    "glue:DeleteSchemaVersions",
    "glue:GetSchemaByDefinition",
    "glue:GetSchemaVersion",
    "glue:GetSchemaVersionsDiff",
    "glue:ListSchemaVersions",
    "glue:CheckSchemaVersionValidity",
    "glue:PutSchemaVersionMetadata",
    "glue:RemoveSchemaVersionMetadata",
    "glue:QuerySchemaVersionMetadata"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetTags",
    "glue:TagResource",
    "glue:UntagResource"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:schema/*",
    "arn:aws:glue:*:*:registry/*"
  ]
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGlueSchemaRegistryReadOnlyAccess

AWSGlueSchemaRegistryReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura al servicio de registro de AWS Glue Schema

Uso de la política

Puede asociar AWSGlueSchemaRegistryReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de noviembre de 2020 a las 00:20 UTC
- Hora de edición: 20 de noviembre de 2020 a las 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
```

```
        "glue:ListSchemaVersions",
        "glue:GetSchemaVersionsDiff",
        "glue:CheckSchemaVersionValidity",
        "glue:QuerySchemaVersionMetadata",
        "glue:GetTags"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGlueServiceNotebookRole

AWSGlueServiceNotebookRole es una [política administrada por AWS](#) para: el rol de servicio de AWS Glue, que permite al cliente administrar el servidor portátil

Uso de la política

Puede asociar AWSGlueServiceNotebookRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 13:37 UTC
- Hora de edición: 09 de octubre de 2023 a las 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue>DeleteDatabase",
        "glue>DeletePartition",
        "glue>DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:CreateConnection",
        "glue:CreateJob",
        "glue>DeleteConnection",
        "glue>DeleteJob",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:UpdateJob",

```

```

    "glue:BatchDeleteConnection",
    "glue:UpdateConnection",
    "glue:GetUserDefinedFunction",
    "glue:UpdateUserDefinedFunction",
    "glue:GetUserDefinedFunctions",
    "glue>DeleteUserDefinedFunction",
    "glue:CreateUserDefinedFunction",
    "glue:BatchGetPartition",
    "glue:BatchDeletePartition",
    "glue:BatchCreatePartition",
    "glue:BatchDeleteTable",
    "glue:UpdateDevEndpoint",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketAcl",
    "codewhisperer:GenerateRecommendations"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::crawler-public*",
    "arn:aws:s3:::aws-glue*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3>DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue*"
  ]
},
{
  "Effect" : "Allow",

```

```
"Action" : [
  "ec2:CreateTags",
  "ec2>DeleteTags"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "aws-glue-service-resource"
    ]
  }
},
"Resource" : [
  "arn:aws:ec2:*:*:network-interface/*",
  "arn:aws:ec2:*:*:security-group/*",
  "arn:aws:ec2:*:*:instance/*"
]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGlueServiceRole

AWSGlueServiceRole es una [política administrada por AWS](#) que: el rol de servicio de AWS Glue que permite el acceso a servicios relacionados, incluidos los registros de EC2, S3 y Cloudwatch

Uso de la política

Puede asociar AWSGlueServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 13:37 UTC
- Hora de edición: 11 de septiembre de 2023 a las 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*/**",
      "arn:aws:s3:::*/**aws-glue-*/**"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::crawler-public*",
      "arn:aws:s3:::aws-glue-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
```

```

    "arn:aws:logs:*:*:*:/aws-glue/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws-glue-service-resource"
      ]
    }
  },
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
}
]
}
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AwsGlueSessionUserRestrictedNotebookPolicy

AwsGlueSessionUserRestrictedNotebookPolicy es una [política administrada por AWS](#) que: proporciona permisos para que los usuarios creen y utilicen solo las sesiones de cuadernos que estén asociadas al usuario. Esta política también incluye permisos para que los usuarios puedan pasar expresamente un rol de sesión de Glue restringido.

Uso de la política

Puede asociar `AwsGlueSessionUserRestrictedNotebookPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de abril de 2022 a las 15:24 UTC
- Hora editada: 22 de noviembre de 2023, 01:32 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
```

```
        "owner"
      ]
    }
  },
  {
    "Sid" : "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"
            ]
        }
    }
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

`AwsGlueSessionUserRestrictedNotebookServiceRole` es una [política administrada por AWS](#) que: proporciona acceso total a todos los recursos de AWS Glue, salvo las sesiones. Permite a los usuarios crear y utilizar solo las sesiones de cuadernos que estén asociadas a esos usuarios. Esta política también incluye otros permisos que necesita AWS Glue para administrar los recursos de Glue en otros servicios de AWS.

Uso de la política

Puede asociar `AwsGlueSessionUserRestrictedNotebookServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de abril de 2022 a las 15:27 UTC
- Hora de edición: 18 de abril de 2022 a las 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
```

```
        "owner"
      ]
    }
  },
  {
    "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/*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AwsGlueSessionUserRestrictedPolicy

AwsGlueSessionUserRestrictedPolicy es una [política administrada por AWS](#) que: concede permisos para que los usuarios creen y utilicen solo las sesiones interactivas que están asociadas al usuario. Esta política también incluye permisos para que los usuarios puedan pasar expresamente un rol de sesión de Glue restringido.

Uso de la política

Puede asociar AwsGlueSessionUserRestrictedPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de abril de 2022 a las 21:31 UTC
- Hora de edición: 14 de abril de 2022 a las 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/owner" : "${aws:userid}"
      },
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "owner"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:RunStatement",
      "glue:GetStatement",
      "glue:ListStatements",
      "glue:CancelStatement",
      "glue:StopSession",
      "glue>DeleteSession",
      "glue:GetSession"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/owner" : "${aws:userid}"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:ListSessions"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "glue:TagResource",

```



```
    "glue:UntagResource",
    "tag:TagResources",
    "tag:UntagResources"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AwsGlueSessionUserRestrictedServiceRole

AwsGlueSessionUserRestrictedServiceRole es una [política administrada por AWS](#) que: proporciona acceso total a todos los recursos de AWS Glue, salvo las sesiones. Permite a los usuarios crear y utilizar solo las sesiones interactivas que están asociadas al usuario. Esta política también incluye otros permisos que necesita AWS Glue para administrar los recursos de Glue en otros servicios de AWS.

Uso de la política

Puede asociar AwsGlueSessionUserRestrictedServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de abril de 2022 a las 21:30 UTC
- Hora de edición: 14 de abril de 2022 a las 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Action" : "glue:*",
    "Resource" : [
      "arn:aws:glue:*:*:catalog/*",
      "arn:aws:glue:*:*:database/*",
      "arn:aws:glue:*:*:table/*",
      "arn:aws:glue:*:*:tableVersion/*",
      "arn:aws:glue:*:*:connection/*",
      "arn:aws:glue:*:*:userDefinedFunction/*",
      "arn:aws:glue:*:*:devEndpoint/*",
      "arn:aws:glue:*:*:job/*",
      "arn:aws:glue:*:*:trigger/*",
      "arn:aws:glue:*:*:crawler/*",
      "arn:aws:glue:*:*:workflow/*",
      "arn:aws:glue:*:*:mlTransform/*",
      "arn:aws:glue:*:*:registry/*",
      "arn:aws:glue:*:*:schema*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateSession"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:session*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/owner" : "${aws:userid}"
      },
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "owner"
        ]
      }
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:RunStatement",
    "glue:GetStatement",
    "glue:ListStatements",
    "glue:CancelStatement",

```

```
    "glue:StopSession",
    "glue>DeleteSession",
    "glue:GetSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/owner" : "${aws:userid}"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:ListSessions"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "glue:TagResource",
    "glue:UntagResource",
    "tag:TagResources",
    "tag:UntagResources"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
    "s3:CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*/**",
    "arn:aws:s3:::*/**aws-glue-*/**"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::crawler-public*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*/aws-glue/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
}
```

```
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "aws-glue-service-resource"
    ]
  }
},
"Resource" : [
  "arn:aws:ec2:*:*:network-interface/*",
  "arn:aws:ec2:*:*:security-group/*",
  "arn:aws:ec2:*:*:instance/*"
]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGrafanaAccountAdministrator

AWSGrafanaAccountAdministrator es una [política administrada por AWS](#) que: brinda acceso dentro de Amazon Grafana para crear y administrar espacios de trabajo para toda la organización.

Uso de la política

Puede asociar AWSGrafanaAccountAdministrator a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de febrero de 2021 a las 00:20 UTC
- Hora de edición: 15 de febrero de 2022 a las 22:36 UTC

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

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaOrganizationAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMGetRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
```

```
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "grafana.amazonaws.com"
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGrafanaConsoleReadOnlyAccess

AWSGrafanaConsoleReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a las operaciones en Grafana de Amazon.

Uso de la política

Puede asociar AWSGrafanaConsoleReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de febrero de 2021 a las 00:10 UTC
- Hora de edición: 15 de febrero de 2022 a las 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGrafanaWorkspacePermissionManagement

AWSGrafanaWorkspacePermissionManagement es una [política administrada por AWS](#) que: proporciona únicamente la posibilidad de actualizar los permisos de usuario y grupo para los espacios de trabajo de Grafana de AWS.

Uso de la política

Puede asociar AWSGrafanaWorkspacePermissionManagement a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de febrero de 2021 a las 00:15 UTC
- Hora de edición: 15 de marzo de 2023 a las 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",

```

```
    "sso:ListProfiles",
    "sso:AssociateProfile",
    "sso:DisassociateProfile",
    "sso:GetProfile",
    "sso:ListProfileAssociations",
    "sso-directory:DescribeUser",
    "sso-directory:DescribeGroup"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGrafanaWorkspacePermissionManagementV2

AWSGrafanaWorkspacePermissionManagementV2 es una [política AWS gestionada](#) que: permite actualizar los permisos de usuario y grupo del IAM Identity Center (iDC) para los espacios de trabajo de Grafana gestionados por Amazon.

Uso de la política

Puede asociar AWSGrafanaWorkspacePermissionManagementV2 a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de enero de 2024 a las 18:39 UTC
- Hora editada: 5 de enero de 2024 a las 18:39 UTC

- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGreengrassFullAccess

AWSGreengrassFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a las acciones de configuración, administración e implementación de AWS Greengrass

Uso de la política

Puede asociar AWSGreengrassFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de mayo de 2017 a las 00:47 UTC
- Hora de edición: 3 de mayo de 2017 a las 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGreengrassReadOnlyAccess

AWSGreengrassReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a las acciones de configuración, administración e implementación de AWS Greengrass

Uso de la política

Puede asociar AWSGreengrassReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 30 de octubre de 2018 a las 16:01 UTC
- Hora de edición: 30 de octubre de 2018 a las 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGreengrassResourceAccessRolePolicy

AWSGreengrassResourceAccessRolePolicy es una [política administrada por AWS](#) que: es una política para el rol de servicio de AWS Greengrass que permite el acceso a servicios relacionados, incluidos AWS Lambda e AWS IoT Things Shadow.

Uso de la política

Puede asociar AWSGreengrassResourceAccessRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de febrero de 2017 a las 21:17 UTC
- Hora de edición: 14 de noviembre de 2018 a las 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGreengrassAccessToShadows",
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Effect" : "Allow",
    }
  ]
}
```



```
"Resource" : [
  "arn:aws:iot:*:*:thing/GG_*",
  "arn:aws:iot:*:*:thing/*-gcm",
  "arn:aws:iot:*:*:thing/*-gda",
  "arn:aws:iot:*:*:thing/*-gci"
],
{
  "Sid" : "AllowGreengrassToDescribeThings",
  "Action" : [
    "iot:DescribeThing"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iot:*:*:thing/*"
},
{
  "Sid" : "AllowGreengrassToDescribeCertificates",
  "Action" : [
    "iot:DescribeCertificate"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iot:*:*:cert/*"
},
{
  "Sid" : "AllowGreengrassToCallGreengrassServices",
  "Action" : [
    "greengrass:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "AllowGreengrassToGetLambdaFunctions",
  "Action" : [
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "AllowGreengrassToGetGreengrassSecrets",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ]
}
```

```
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
  },
  {
    "Sid" : "AllowGreengrassAccessToS3Objects",
    "Action" : [
      "s3:GetObject"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:s3::*Greengrass*",
      "arn:aws:s3::*GreenGrass*",
      "arn:aws:s3::*greengrass*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Sid" : "AllowGreengrassAccessToS3BucketLocation",
    "Action" : [
      "s3:GetBucketLocation"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
    "Action" : [
      "sagemaker:DescribeTrainingJob"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:sagemaker:*:*:training-job/*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSGroundStationAgentInstancePolicy

AWSGroundStationAgentInstancePolicy es una [política administrada por AWS](#) que: proporciona a la instancia de punto de conexión de Dataflow los permisos para usar el Agente de AWS Ground Station

Uso de la política

Puede asociar AWSGroundStationAgentInstancePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de marzo de 2023 a las 15:23 UTC
- Hora de edición: 29 de marzo de 2023 a las 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSHealth_EventProcessorServiceRolePolicy

AWSHealth_EventProcessorServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWSHealth active la característica de procesador de eventos de Health.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de enero de 2023 a las 19:24 UTC
- Hora de edición: 13 de enero de 2023 a las 19:24 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSHealthFullAccess

AWSHealthFullAccess es una [política administrada por AWS](#) que: permite el acceso total a las API y notificaciones de AWS Health y al Personal Health Dashboard

Uso de la política

Puede asociar AWSHealthFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de diciembre de 2016 a las 12:30 UTC
- Hora de edición: 16 de noviembre de 2020 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "health.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "health:*",
      "organizations:ListAccounts",
      "organizations:ListParents",
      "organizations:DescribeAccount",
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "health.amazonaws.com"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSHealthImagingFullAccess

AWSHealthImagingFullAccess es una [política administrada por AWS](#) que: proporciona acceso total al servicio AWS Health Imaging.

Uso de la política

Puede asociar AWSHealthImagingFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de julio de 2023 a las 23:39 UTC
- Hora de edición: 25 de julio de 2023 a las 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "medical-imaging.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSHealthImagingReadOnlyAccess

AWSHealthImagingReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio AWS Health Imaging.

Uso de la política

Puede asociar AWSHealthImagingReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de julio de 2023 a las 23:40 UTC
- Hora de edición: 1 de agosto de 2023 a las 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIAMIdentityCenterAllowListForIdentityContext

AWSIAMIdentityCenterAllowListForIdentityContext es una [política administrada por AWS](#) que: brinda la lista de acciones permitidas para los roles asumidos con el contexto de identidad del IAM Identity Center. AWS Security Token Service (STS de AWS) asocia automáticamente esta política a los roles asumidos. El contexto de identidad se transmite como ProvidedContext.

Uso de la política

Puede asociar AWSIAMIdentityCenterAllowListForIdentityContext a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de noviembre de 2023 a las 15:21 UTC
- Hora editada: 25 de noviembre de 2023 a las 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIdentitySyncFullAccess

AWSIdentitySyncFullAccess es una [política administrada por AWS](#) que: concede acceso total al servicio Identity Sync

Uso de la política

Puede asociar AWSIdentitySyncFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de marzo de 2022 a las 23:29 UTC
- Hora de edición: 23 de marzo de 2022 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication"
      ],
      "Resource" : "arn:*:ds:*:*:*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile",
        "identity-sync:CreateSyncProfile",
        "identity-sync:GetSyncProfile",
        "identity-sync:StartSync",
        "identity-sync:StopSync",
        "identity-sync:CreateSyncFilter",
        "identity-sync>DeleteSyncFilter",
        "identity-sync:ListSyncFilters",
        "identity-sync:CreateSyncTarget",
```

```
        "identity-sync:DeleteSyncTarget",
        "identity-sync:GetSyncTarget",
        "identity-sync:UpdateSyncTarget"
    ],
    "Resource" : "arn:*:identity-sync:*:*:*/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIdentitySyncReadOnlyAccess

AWSIdentitySyncReadOnlyAccess es una [política administrada por AWS](#) que: permite el acceso de solo lectura al servicio Identity Sync

Uso de la política

Puede asociar AWSIdentitySyncReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de marzo de 2022 a las 23:29 UTC
- Hora de edición: 23 de marzo de 2022 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*/*/*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSImageBuilderFullAccess

AWSImageBuilderFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todas las acciones de Image Builder de AWS y acceso limitado a los recursos a los servicios de AWS relacionados.

Uso de la política

Puede asociar AWSImageBuilderFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de diciembre de 2019 a las 18:25 UTC
- Hora de edición: 13 de abril de 2021 a las 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/AWSServiceRoleForImageBuilder"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*imagebuilder*",
        "arn:aws:iam::*:role/*imagebuilder*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*:imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    }
  ]

```

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSImageBuilderReadOnlyAccess

AWSImageBuilderReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a todas las acciones de Image Builder de AWS.

Uso de la política

Puede asociar AWSImageBuilderReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de diciembre de 2019 a las 22:29 UTC
- Hora de edición: 19 de diciembre de 2019 a las 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:Get*",
        "imagebuilder:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/AWSServiceRoleForImageBuilder"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSImportExportFullAccess

`AWSImportExportFullAccess` es una [política administrada por AWS](#) que: brinda acceso de lectura y escritura a los trabajos creados en la Cuenta de AWS.

Uso de la política

Puede asociar `AWSImportExportFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSImportExportReadOnlyAccess

AWSImportExportReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a los trabajos creados en la Cuenta de AWS.

Uso de la política

Puede asociar AWSImportExportReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ]
    }
  ]
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

AWSIncidentManagerIncidentAccessServiceRolePolicy es una [política AWS gestionada](#) que: otorga al administrador de incidentes permisos para llamar a otros AWS servicios como parte de la gestión de un incidente.

Uso de la política

Puede asociar AWSIncidentManagerIncidentAccessServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de noviembre de 2023 a las 00:01 UTC
- Hora editada: 20 de febrero de 2024 a las 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSIncidentManagerResolverAccess

`AWSIncidentManagerResolverAccess` es una [política administrada por AWS](#) que: otorga permisos para iniciar, ver y actualizar incidentes con acceso total a los eventos personalizados de

la cronología, y a los elementos relacionados. Asigne esta política a los usuarios que crearán y resolverán los incidentes.

Uso de la política

Puede asociar `AWSIncidentManagerResolverAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de mayo de 2021 a las 06:12 UTC
- Hora de edición: 10 de mayo de 2021 a las 06:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
    "ssm-incidents:ListResponsePlans",
    "ssm-incidents:GetResponsePlan"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IncidentRecordResolverPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm-incidents:ListIncidentRecords",
    "ssm-incidents:GetIncidentRecord",
    "ssm-incidents:UpdateIncidentRecord",
    "ssm-incidents:ListTimelineEvents",
    "ssm-incidents:CreateTimelineEvent",
    "ssm-incidents:GetTimelineEvent",
    "ssm-incidents:UpdateTimelineEvent",
    "ssm-incidents>DeleteTimelineEvent",
    "ssm-incidents:ListRelatedItems",
    "ssm-incidents:UpdateRelatedItems"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIncidentManagerServiceRolePolicy

AWSIncidentManagerServiceRolePolicy es una [política administrada por AWS](#) que: otorga permiso al administrador de incidentes para gestionar los registros de incidentes y los recursos relacionados en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de mayo de 2021 a las 03:34 UTC
- Hora de edición: 5 de diciembre de 2022 a las 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
    ],
    "Resource" : "*"
},
{
    "Sid" : "IncidentEngagementPermissions",
    "Effect" : "Allow",
    "Action" : "ssm-contacts:StartEngagement",
    "Resource" : "*"
},
{
    "Sid" : "PutMetricDataPermission",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "cloudwatch:namespace" : "AWS/IncidentManager"
        }
    }
}
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoT1ClickFullAccess

AWSIoT1ClickFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS IoT 1-Click.

Uso de la política

Puede asociar AWSIoT1ClickFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de mayo de 2018 a las 22:10 UTC
- Hora de edición: 11 de mayo de 2018 a las 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoT1ClickReadOnlyAccess

AWSIoT1ClickReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AWS IoT 1-Click.

Uso de la política

Puede asociar AWSIoT1ClickReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de mayo de 2018 a las 21:49 UTC
- Hora de edición: 11 de mayo de 2018 a las 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTAnalyticsFullAccess

AWSIoTAnalyticsFullAccess es una [política administrada por AWS](#) que: brinda acceso total a IoT Analytics.

Uso de la política

Puede asociar AWSIoTAnalyticsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de junio de 2018 a las 23:02 UTC
- Hora de edición: 18 de junio de 2018 a las 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTAnalyticsReadOnlyAccess

AWSIoTAnalyticsReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a IoT Analytics.

Uso de la política

Puede asociar AWSIoTAnalyticsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de junio de 2018 a las 21:37 UTC

- Hora de edición: 18 de junio de 2018 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTConfigAccess

AWSIoTConfigAccess es una [política administrada por AWS](#) que: brinda acceso total a las acciones de configuración de AWS IoT

Uso de la política

Puede asociar AWSIoTConfigAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de octubre de 2015 a las 21:52 UTC
- Hora de edición: 27 de septiembre de 2019 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
```

```
"iot:CancelJobExecution",
"iot:ClearDefaultAuthorizer",
"iot:CreateAuthorizer",
"iot:CreateCertificateFromCsr",
"iot:CreateJob",
"iot:CreateKeysAndCertificate",
"iot:CreateOTAUpdate",
"iot:CreatePolicy",
"iot:CreatePolicyVersion",
"iot:CreateRoleAlias",
"iot:CreateStream",
"iot:CreateThing",
"iot:CreateThingGroup",
"iot:CreateThingType",
"iot:CreateTopicRule",
"iot>DeleteAuthorizer",
"iot>DeleteCACertificate",
"iot>DeleteCertificate",
"iot>DeleteJob",
"iot>DeleteJobExecution",
"iot>DeleteOTAUpdate",
"iot>DeletePolicy",
"iot>DeletePolicyVersion",
"iot>DeleteRegistrationCode",
"iot>DeleteRoleAlias",
"iot>DeleteStream",
"iot>DeleteThing",
"iot>DeleteThingGroup",
"iot>DeleteThingType",
"iot>DeleteTopicRule",
"iot>DeleteV2LoggingLevel",
"iot:DeprecateThingType",
"iot:DescribeAuthorizer",
"iot:DescribeCACertificate",
"iot:DescribeCertificate",
"iot:DescribeDefaultAuthorizer",
"iot:DescribeEndpoint",
"iot:DescribeEventConfigurations",
"iot:DescribeIndex",
"iot:DescribeJob",
"iot:DescribeJobExecution",
"iot:DescribeRoleAlias",
"iot:DescribeStream",
"iot:DescribeThing",
```

```
"iot:DescribeThingGroup",
"iot:DescribeThingRegistrationTask",
"iot:DescribeThingType",
"iot:DetachPolicy",
"iot:DetachPrincipalPolicy",
"iot:DetachThingPrincipal",
"iot:DisableTopicRule",
"iot:EnableTopicRule",
"iot:GetEffectivePolicies",
"iot:GetIndexingConfiguration",
"iot:GetJobDocument",
"iot:GetLoggingOptions",
"iot:GetOTAUpdate",
"iot:GetPolicy",
"iot:GetPolicyVersion",
"iot:GetRegistrationCode",
"iot:GetTopicRule",
"iot:GetV2LoggingOptions",
"iot:ListAttachedPolicies",
"iot:ListAuthorizers",
"iot:ListCACertificates",
"iot:ListCertificates",
"iot:ListCertificatesByCA",
"iot:ListIndices",
"iot:ListJobExecutionsForJob",
"iot:ListJobExecutionsForThing",
"iot:ListJobs",
"iot:ListOTAUpdates",
"iot:ListOutgoingCertificates",
"iot:ListPolicies",
"iot:ListPolicyPrincipals",
"iot:ListPolicyVersions",
"iot:ListPrincipalPolicies",
"iot:ListPrincipalThings",
"iot:ListRoleAliases",
"iot:ListStreams",
"iot:ListTargetsForPolicy",
"iot:ListThingGroups",
"iot:ListThingGroupsForThing",
"iot:ListThingPrincipals",
"iot:ListThingRegistrationTaskReports",
"iot:ListThingRegistrationTasks",
"iot:ListThings",
"iot:ListThingsInThingGroup",
```

```
"iot:ListThingTypes",
"iot:ListTopicRules",
"iot:ListV2LoggingLevels",
"iot:RegisterCACertificate",
"iot:RegisterCertificate",
"iot:RegisterThing",
"iot:RejectCertificateTransfer",
"iot:RemoveThingFromThingGroup",
"iot:ReplaceTopicRule",
"iot:SearchIndex",
"iot:SetDefaultAuthorizer",
"iot:SetDefaultPolicyVersion",
"iot:SetLoggingOptions",
"iot:SetV2LoggingLevel",
"iot:SetV2LoggingOptions",
"iot:StartThingRegistrationTask",
"iot:StopThingRegistrationTask",
"iot:TestAuthorization",
"iot:TestInvokeAuthorizer",
"iot:TransferCertificate",
"iot:UpdateAuthorizer",
"iot:UpdateCACertificate",
"iot:UpdateCertificate",
"iot:UpdateEventConfigurations",
"iot:UpdateIndexingConfiguration",
"iot:UpdateRoleAlias",
"iot:UpdateStream",
"iot:UpdateThing",
"iot:UpdateThingGroup",
"iot:UpdateThingGroupsForThing",
"iot:UpdateAccountAuditConfiguration",
"iot:DescribeAccountAuditConfiguration",
"iot>DeleteAccountAuditConfiguration",
"iot:StartOnDemandAuditTask",
"iot:CancelAuditTask",
"iot:DescribeAuditTask",
"iot:ListAuditTasks",
"iot>CreateScheduledAudit",
"iot:UpdateScheduledAudit",
"iot>DeleteScheduledAudit",
"iot:DescribeScheduledAudit",
"iot:ListScheduledAudits",
"iot:ListAuditFindings",
"iot>CreateSecurityProfile",
```

```
    "iot:DescribeSecurityProfile",
    "iot:UpdateSecurityProfile",
    "iot>DeleteSecurityProfile",
    "iot:AttachSecurityProfile",
    "iot:DetachSecurityProfile",
    "iot:ListSecurityProfiles",
    "iot:ListSecurityProfilesForTarget",
    "iot:ListTargetsForSecurityProfile",
    "iot:ListActiveViolations",
    "iot:ListViolationEvents",
    "iot:ValidateSecurityProfileBehaviors"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTConfigReadOnlyAccess

AWSIoTConfigReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a las acciones de configuración de AWS IoT

Uso de la política

Puede asociar AWSIoTConfigReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de octubre de 2015 a las 21:52 UTC

- Hora de edición: 27 de septiembre de 2019 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
```



```
"iot:GetTopicRule",
"iot:GetV2LoggingOptions",
"iot:ListAttachedPolicies",
"iot:ListAuthorizers",
"iot:ListCACertificates",
"iot:ListCertificates",
"iot:ListCertificatesByCA",
"iot:ListIndices",
"iot:ListJobExecutionsForJob",
"iot:ListJobExecutionsForThing",
"iot:ListJobs",
"iot:ListOTAUpdates",
"iot:ListOutgoingCertificates",
"iot:ListPolicies",
"iot:ListPolicyPrincipals",
"iot:ListPolicyVersions",
"iot:ListPrincipalPolicies",
"iot:ListPrincipalThings",
"iot:ListRoleAliases",
"iot:ListStreams",
"iot:ListTargetsForPolicy",
"iot:ListThingGroups",
"iot:ListThingGroupsForThing",
"iot:ListThingPrincipals",
"iot:ListThingRegistrationTaskReports",
"iot:ListThingRegistrationTasks",
"iot:ListThings",
"iot:ListThingsInThingGroup",
"iot:ListThingTypes",
"iot:ListTopicRules",
"iot:ListV2LoggingLevels",
"iot:SearchIndex",
"iot:TestAuthorization",
"iot:TestInvokeAuthorizer",
"iot:DescribeAccountAuditConfiguration",
"iot:DescribeAuditTask",
"iot:ListAuditTasks",
"iot:DescribeScheduledAudit",
"iot:ListScheduledAudits",
"iot:ListAuditFindings",
"iot:DescribeSecurityProfile",
"iot:ListSecurityProfiles",
"iot:ListSecurityProfilesForTarget",
"iot:ListTargetsForSecurityProfile",
```

```
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDataAccess

AWSIoTDataAccess es una [política administrada por AWS](#) que: concede acceso total a las acciones de mensajería de AWS IoT

Uso de la política

Puede asociar AWSIoTDataAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de octubre de 2015 a las 21:51 UTC
- Hora de edición: 23 de junio de 2021 a las 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
        "iot:Receive",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow",
        "iot>DeleteThingShadow",
        "iot:ListNamedShadowsForThing"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction es una [política administrada por AWS](#) que: proporciona acceso de escritura a los grupos de cosas de IoT,

y acceso de lectura a los certificados de IoT para la ejecución de la acción de mitigación

`ADD_THINGS_TO_THING_GROUP`

Uso de la política

Puede asociar `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:55 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceDefenderAudit

`AWSIoTDeviceDefenderAudit` es una [política administrada por AWS](#) que: proporciona acceso de lectura para el IoT y los recursos relacionados

Uso de la política

Puede asociar `AWSIoTDeviceDefenderAudit` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de julio de 2018 a las 21:17 UTC
- Hora de edición: 25 de noviembre de 2019 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction es una [política administrada por AWS](#) que: proporciona acceso para habilitar el registro de IoT, y así ejecutar la acción de mitigación ENABLE_IOT_LOGGING

Uso de la política

Puede asociar AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:04 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Action" : [
      "iot:SetV2LoggingOptions"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "iot.amazonaws.com"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction es una [política administrada por AWS](#) que: proporciona a los mensajes acceso de publicación al tema de SNS para ejecutar la acción de mitigación PUBLISH_FINDING_TO_SNS

Uso de la política

Puede asociar `AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:04 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction es una [política administrada por AWS](#) que: concede acceso de escritura a las políticas de IoT para ejecutar la acción de mitigación REPLACE_DEFAULT_POLICY_VERSION

Uso de la política

Puede asociar AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:04 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

AWSIoTDeviceDefenderUpdateCACertMitigationAction es una [política administrada por AWS](#) que: proporciona acceso de escritura a los certificados de CA de IoT para ejecutar la acción de mitigación UPDATE_CA_CERTIFICATE

Uso de la política

Puede asociar AWSIoTDeviceDefenderUpdateCACertMitigationAction a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:05 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction es una [política administrada por AWS](#) que: concede acceso de escritura a los certificados de IoT para ejecutar la acción de mitigación UPDATE_DEVICE_CERTIFICATE

Uso de la política

Puede asociar AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:06 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "iot:UpdateCertificate"
  ],
  "Resource" : [
    "*"
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

AWSIoTDeviceTesterForFreeRTOSFullAccess es una [política administrada por AWS](#) que: permite a IoT Device Tester de AWS ejecutar el conjunto de calificaciones FreeRTOS, al permitir el acceso a servicios como IoT, S3 e IAM

Uso de la política

Puede asociar AWSIoTDeviceTesterForFreeRTOSFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de febrero de 2020 a las 20:33 UTC
- Hora de edición: 10 de agosto de 2023 a las 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteThing",
        "iot:AttachThingPrincipal",
        "iot:DeleteCertificate",
        "iot:GetRegistrationCode",
        "iot:CreatePolicy",
        "iot:UpdateCACertificate",
        "s3:ListBucket",
        "iot:DescribeEndpoint",
        "iot:CreateOTAUpdate",
        "iot:CreateStream",
        "signer:ListSigningJobs",
        "acm:ListCertificates",
        "iot:CreateKeysAndCertificate",
        "iot:UpdateCertificate",
        "iot:CreateCertificateFromCsr",

```

```

    "iot:DetachThingPrincipal",
    "iot:RegisterCACertificate",
    "iot:CreateThing",
    "iam:ListRoles",
    "iot:RegisterCertificate",
    "iot>DeleteCACertificate",
    "signer:PutSigningProfile",
    "s3:ListAllMyBuckets",
    "signer:ListSigningPlatforms",
    "iot-device-tester:SendMetrics",
    "iot-device-tester:SupportedVersion",
    "iot-device-tester:LatestIdt",
    "iot-device-tester:CheckVersion",
    "iot-device-tester:DownloadTestSuite"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor2",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "signer:StartSigningJob",
    "acm:GetCertificate",
    "signer:DescribeSigningJob",
    "s3:CreateBucket",
    "execute-api:Invoke",
    "s3>DeleteBucket",
    "s3:PutBucketVersioning",
    "signer:CancelSigningProfile"
  ],
  "Resource" : [
    "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
    "arn:aws:signer:*:*/signing-profiles/*",
    "arn:aws:signer:*:*/signing-jobs/*",
    "arn:aws:iam:*:*/role/idt-*",
    "arn:aws:acm:*:*/certificate/*",
    "arn:aws:s3:::idt-*",
    "arn:aws:s3:::afr-ota*"
  ]
},
{
  "Sid" : "VisualEditor3",
  "Effect" : "Allow",

```



```

    "Action" : [
      "iot:DeleteStream",
      "iot:DeleteCertificate",
      "iot:AttachPolicy",
      "iot:DetachPolicy",
      "iot:DeletePolicy",
      "s3:ListBucketVersions",
      "iot:UpdateCertificate",
      "iot:GetOTAUpdate",
      "iot:DeleteOTAUpdate",
      "iot:DescribeJobExecution"
    ],
    "Resource" : [
      "arn:aws:s3:::afr-ota*",
      "arn:aws:iot:*:*:thinggroup/idt*",
      "arn:aws:iam:*:*:role/idt-*"
    ]
  },
  {
    "Sid" : "VisualEditor4",
    "Effect" : "Allow",
    "Action" : [
      "iot:DeleteCertificate",
      "iot:AttachPolicy",
      "iot:DetachPolicy",
      "s3:DeleteObjectVersion",
      "iot:DeleteOTAUpdate",
      "s3:PutObject",
      "s3:GetObject",
      "iot:DeleteStream",
      "iot:DeletePolicy",
      "s3:DeleteObject",
      "iot:UpdateCertificate",
      "iot:GetOTAUpdate",
      "s3:GetObjectVersion",
      "iot:DescribeJobExecution"
    ],
    "Resource" : [
      "arn:aws:s3:::afr-ota/*",
      "arn:aws:s3:::idt-/*",
      "arn:aws:iot:*:*:policy/idt*",
      "arn:aws:iam:*:*:role/idt-*",
      "arn:aws:iot:*:*:otaupdate/idt*",
      "arn:aws:iot:*:*:thing/idt*"
    ]
  }

```

```

        "arn:aws:iot:*:*:cert/*",
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:stream/*"
    ]
},
{
    "Sid" : "VisualEditor5",
    "Effect" : "Allow",
    "Action" : [
        "s3:PutObject",
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::afr-ota/*",
        "arn:aws:s3:::idt-*/*"
    ]
},
{
    "Sid" : "VisualEditor6",
    "Effect" : "Allow",
    "Action" : [
        "iot:CancelJobExecution"
    ],
    "Resource" : [
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:thing/idt*"
    ]
},
{
    "Sid" : "VisualEditor7",
    "Effect" : "Allow",
    "Action" : [
        "ec2:TerminateInstances"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
    }
},
{

```

```
"Sid" : "VisualEditor8",
"Effect" : "Allow",
"Action" : [
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2>DeleteSecurityGroup"
],
"Resource" : [
  "arn:aws:ec2:*:*:security-group/*"
],
"Condition" : {
  "StringEquals" : {
    "ec2:ResourceTag/Owner" : "IoTDeviceTester"
  }
}
},
{
  "Sid" : "VisualEditor9",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Owner" : "IoTDeviceTester"
    }
  }
}
},
{
  "Sid" : "VisualEditor10",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:network-interface/*",
```

```
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "VisualEditor11",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Owner" : "IoTDeviceTester"
    }
  }
},
{
  "Sid" : "VisualEditor12",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "ssm:DescribeParameters",
    "ssm:GetParameters"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor13",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "Owner"
      ]
    }
  }
}
```

```
    },
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances",
        "CreateSecurityGroup"
      ]
    }
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTDeviceTesterForGreengrassFullAccess

AWSIoTDeviceTesterForGreengrassFullAccess es una [política administrada por AWS](#) que: permite que AWS IoT Device Tester ejecute el conjunto de calificaciones de AWS Greengrass, al permitir el acceso a servicios relacionados, como Lambda, IoT, la Puerta de enlace de la API e IAM

Uso de la política

Puede asociar AWSIoTDeviceTesterForGreengrassFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de febrero de 2020 a las 21:21 UTC
- Hora de edición: 25 de junio de 2020 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "iot>DeleteCertificate",
        "lambda>DeleteFunction",
        "execute-api:Invoke",
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:lambda::*:function:idt-*",
        "arn:aws:iot::*:cert/*"
      ]
    }
  ]
}
```

```
},
{
  "Sid" : "VisualEditor3",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateThing",
    "iot>DeleteThing"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor4",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachPolicy",
    "iot:DetachPolicy",
    "iot>DeletePolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor5",
  "Effect" : "Allow",
  "Action" : [
    "iot>CreateJob",
    "iot:DescribeJob",
    "iot:DescribeJobExecution",
    "iot>DeleteJob"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/idt-*",
    "arn:aws:iot:*:*:job/*"
  ]
},
{
  "Sid" : "VisualEditor6",
  "Effect" : "Allow",
  "Action" : [
```

```

    "iot:DescribeEndpoint",
    "greengrass:*",
    "iam:ListAttachedRolePolicies",
    "iot:CreatePolicy",
    "iot:GetThingShadow",
    "iot:CreateKeysAndCertificate",
    "iot:ListThings",
    "iot:UpdateThingShadow",
    "iot:CreateCertificateFromCsr",
    "iot-device-tester:SendMetrics",
    "iot-device-tester:SupportedVersion",
    "iot-device-tester:LatestIdt",
    "iot-device-tester:CheckVersion",
    "iot-device-tester:DownloadTestSuite"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor7",
  "Effect" : "Allow",
  "Action" : [
    "iot:DetachThingPrincipal",
    "iot:AttachThingPrincipal"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor8",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:DeleteObjectVersion",
    "s3:ListBucketVersions",
    "s3:CreateBucket",
    "s3:DeleteObject",
    "s3:DeleteBucket"
  ],
  "Resource" : "arn:aws:s3:::idt*"
}
]

```


}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTEventsFullAccess

AWSIoTEventsFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a IoT Events.

Uso de la política

Puede asociar AWSIoTEventsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de enero de 2019 a las 22:51 UTC
- Hora de edición: 10 de enero de 2019 a las 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTEventsReadOnlyAccess

AWSIoTEventsReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a IoT Events.

Uso de la política

Puede asociar AWSIoTEventsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de enero de 2019 a las 22:50 UTC

- Hora de edición: 23 de septiembre de 2019 a las 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoT FleetHub Federation Access

AWSIoT FleetHub Federation Access es una [política administrada por AWS](#) que: concede Acceso de federación para las aplicaciones de IoT Fleet Hub

Uso de la política

Puede asociar AWSIoT FleetHub Federation Access a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 15 de diciembre de 2020 a las 08:08 UTC
- Hora de edición: 4 de abril de 2022 a las 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoT FleetHub Federation Access`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeIndex",
        "iot:DescribeThingGroup",
        "iot:GetBucketsAggregation",
        "iot:GetCardinality",
        "iot:GetIndexingConfiguration",
        "iot:GetPercentiles",
        "iot:GetStatistics",
        "iot:SearchIndex",

```

```
    "iot:CreateFleetMetric",
    "iot:ListFleetMetrics",
    "iot>DeleteFleetMetric",
    "iot:DescribeFleetMetric",
    "iot:UpdateFleetMetric",
    "iot:DescribeCustomMetric",
    "iot:ListCustomMetrics",
    "iot:ListDimensions",
    "iot:ListMetricValues",
    "iot:ListThingGroups",
    "iot:ListThingsInThingGroup",
    "iot:ListJobTemplates",
    "iot:DescribeJobTemplate",
    "iot:ListJobs",
    "iot:CreateJob",
    "iot:CancelJob",
    "iot:DescribeJob",
    "iot:ListJobExecutionsForJob",
    "iot:ListJobExecutionsForThing",
    "iot:DescribeJobExecution",
    "iot:ListSecurityProfiles",
    "iot:DescribeSecurityProfile",
    "iot:ListActiveViolations",
    "iot:GetThingShadow",
    "iot:ListNamedShadowsForThing",
    "iot:CancelJobExecution",
    "iot:DescribeEndpoint",
    "iotfleethub:DescribeApplication",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:ListSubscriptionsByTopic",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ]
},
```

```
    "Resource" : "arn:aws:sns:*:*:iotfleethub*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch>DeleteAlarms",
      "cloudwatch:DescribeAlarmHistory"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoT Fleetwise Service Role Policy

AWSIoT Fleetwise Service Role Policy es una [política administrada por AWS](#) que: concede permisos a los recursos de AWS y metadatos utilizados o gestionados por AWSIoT FleetWise para características auxiliares

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de septiembre de 2022 a las 23:27 UTC

- Hora de edición: 21 de septiembre de 2022 a las 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTfleetwiseServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTFullAccess

AWSIoTFullAccess es una [política administrada por AWS](#) que: brinda acceso total a las acciones de configuración y mensajería de AWS IoT

Uso de la política

Puede asociar AWSIoTFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de octubre de 2015 a las 15:19 UTC
- Hora de edición: 19 de mayo de 2022 a las 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTLogging

AWSIoTLogging es una [política administrada por AWS](#) que: permite la creación de grupos de registro de los Registros de Amazon CloudWatch y la transmisión de registros a los grupos

Uso de la política

Puede asociar AWSIoTLogging a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 8 de octubre de 2015 a las 15:17 UTC
- Hora de edición: 8 de octubre de 2015 a las 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:PutMetricFilter",
      "logs:PutRetentionPolicy",
      "logs:GetLogEvents",
      "logs>DeleteLogStream"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTOTAUpdate

AWSIoTOTAUpdate es una [política administrada por AWS](#) que: permite acceso para crear un trabajo de AWS IoT y describir el trabajo del firmante de código de AWS

Uso de la política

Puede asociar AWSIoTOTAUpdate a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 20 de diciembre de 2017 a las 20:36 UTC
- Hora de edición: 20 de diciembre de 2017 a las 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTRoboRunnerFullAccess

`AWSIoTRoboRunnerFullAccess` es una [política administrada por AWS](#) que: otorga permisos de acceso total a AWS IoT RoboRunner.

Uso de la política

Puede asociar `AWSIoTRoboRunnerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2021 a las 03:54 UTC
- Hora de edición: 23 de febrero de 2023 a las 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "iotroborunner.amazonaws.com"
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTRoboRunnerReadOnly

AWSIoTRoboRunnerReadOnly es una [política administrada por AWS](#) que: otorga permisos que brindan acceso de solo lectura a AWS IoT RoboRunner.

Uso de la política

Puede asociar AWSIoTRoboRunnerReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2021 a las 03:43 UTC
- Hora de edición: 16 de noviembre de 2022 a las 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTRoboRunnerServiceRolePolicy

AWSIoTRoboRunnerServiceRolePolicy es una [política administrada por AWS](#) que: permite a AWS IoT RoboRunner gestionar los recursos de AWS asociados en nombre del cliente.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de febrero de 2023 a las 16:56 UTC
- Hora de edición: 21 de febrero de 2023 a las 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTRuleActions

AWSIoTRuleActions es una [política administrada por AWS](#) que: permite el acceso a todos los servicios de AWS compatibles con las acciones de reglas de AWS IoT

Uso de la política

Puede asociar AWSIoTRuleActions a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 8 de octubre de 2015 a las 15:14 UTC
- Hora de edición: 16 de enero de 2018 a las 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Effect" : "Allow",
"Action" : [
  "dynamodb:PutItem",
  "kinesis:PutRecord",
  "iot:Publish",
  "s3:PutObject",
  "sns:Publish",
  "sqs:SendMessage*",
  "cloudwatch:SetAlarmState",
  "cloudwatch:PutMetricData",
  "es:ESHttpPut",
  "firehose:PutRecord"
],
"Resource" : "*"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTSiteWiseConsoleFullAccess

AWSIoTSiteWiseConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total para gestionar AWS IoT SiteWise mediante la AWS Management Console. Tenga en cuenta que esta política también permite crear y enumerar los almacenes de datos utilizados con AWS IoT SiteWise (por ejemplo, AWS IoT Analytics). A su vez, permite acceder a enumerar y ver los recursos de AWS IoT Greengrass, enumerar y modificar los secretos de AWS Secrets Manager, recuperar sombras ocultas de AWS IoT, enumerar recursos con etiquetas específicas, y crear y usar un rol vinculado a un servicio para AWS IoT SiteWise.

Uso de la política

Puede asociar AWSIoTSiteWiseConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 31 de mayo de 2019 a las 21:37 UTC
- Hora de edición: 31 de mayo de 2019 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "iotsitewise:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iotanalytics:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Create*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:GetThingShadow"
      ],
      "Effect" : "Allow",
```

```

    "Resource" : "*"
  },
  {
    "Action" : [
      "greengrass:GetGroup",
      "greengrass:GetGroupVersion",
      "greengrass:GetCoreDefinitionVersion",
      "greengrass:ListGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "secretsmanager:ListSecrets",
      "secretsmanager:CreateSecret"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "secretsmanager:UpdateSecret"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
  },
  {
    "Action" : [
      "tag:GetResources"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/AWSServiceRoleForIoTSiteWise*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
      }
    }
  }

```

```
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "iotsitewise.amazonaws.com"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTSiteWiseFullAccess

AWSIoTSiteWiseFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a IoT SiteWise.

Uso de la política

Puede asociar AWSIoTSiteWiseFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 4 de diciembre de 2018 a las 20:53 UTC
- Hora de edición: 4 de diciembre de 2018 a las 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTSiteWiseMonitorPortalAccess

AWSIoTSiteWiseMonitorPortalAccess es una [política administrada por AWS](#) que: concede permisos para acceder a los activos de AWS IoT SiteWise y a los datos de los activos, crear recursos de AWS IoT SiteWise Monitor y enumerar los usuarios de AWS SSO.

Uso de la política

Puede asociar AWSIoTSiteWiseMonitorPortalAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de mayo de 2020 a las 20:01 UTC
- Hora de edición: 19 de mayo de 2020 a las 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise>DeleteProject",
        "iotsitewise:ListProjects",
```

```

    "iotsitewise:BatchAssociateProjectAssets",
    "iotsitewise:BatchDisassociateProjectAssets",
    "iotsitewise:ListProjectAssets",
    "iotsitewise:CreateDashboard",
    "iotsitewise:DescribeDashboard",
    "iotsitewise:UpdateDashboard",
    "iotsitewise>DeleteDashboard",
    "iotsitewise:ListDashboards",
    "iotsitewise:CreateAccessPolicy",
    "iotsitewise:DescribeAccessPolicy",
    "iotsitewise:UpdateAccessPolicy",
    "iotsitewise>DeleteAccessPolicy",
    "iotsitewise:ListAccessPolicies",
    "iotsitewise:DescribeAsset",
    "iotsitewise:ListAssets",
    "iotsitewise:ListAssociatedAssets",
    "iotsitewise:DescribeAssetProperty",
    "iotsitewise:GetAssetPropertyValue",
    "iotsitewise:GetAssetPropertyValueHistory",
    "iotsitewise:GetAssetPropertyAggregates",
    "sso-directory:DescribeUsers"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

AWSIoTSiteWiseMonitorServiceRolePolicy es una [política administrada por AWS](#) que presenta un rol que otorga a AWS IoT SiteWise permisos de monitoreo para acceder a los activos y

las propiedades de los activos de AWS IoT SiteWise, y para crear proyectos, paneles y políticas de acceso de AWS IoT SiteWise a través de los portales de AWS IoT SiteWise.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2019 a las 00:59 UTC
- Hora de edición: 13 de diciembre de 2019 a las 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise>DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
```



```
    "iotsitewise:BatchDisassociateProjectAssets",
    "iotsitewise:ListProjectAssets",
    "iotsitewise:CreateDashboard",
    "iotsitewise:DescribeDashboard",
    "iotsitewise:UpdateDashboard",
    "iotsitewise>DeleteDashboard",
    "iotsitewise:ListDashboards",
    "iotsitewise:CreateAccessPolicy",
    "iotsitewise:DescribeAccessPolicy",
    "iotsitewise:UpdateAccessPolicy",
    "iotsitewise>DeleteAccessPolicy",
    "iotsitewise:ListAccessPolicies",
    "iotsitewise:DescribeAsset",
    "iotsitewise:ListAssets",
    "iotsitewise:ListAssociatedAssets",
    "iotsitewise:DescribeAssetProperty",
    "iotsitewise:GetAssetPropertyValue",
    "iotsitewise:GetAssetPropertyValueHistory",
    "iotsitewise:GetAssetPropertyAggregates",
    "sso-directory:DescribeUsers"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTSiteWiseReadOnlyAccess

AWSIoTSiteWiseReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a IoT SiteWise.

Uso de la política

Puede asociar AWSIoTSiteWiseReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de diciembre de 2018 a las 20:55 UTC
- Hora de edición: 16 de septiembre de 2022 a las 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTThingsRegistration

AWSIoTThingsRegistration es una [política administrada por AWS](#) que: permite a los usuarios registrar cosas de forma masiva mediante la API StartThingRegistrationTask de AWS IoT

Uso de la política

Puede asociar AWSIoTThingsRegistration a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2017 a las 20:21 UTC
- Hora de edición: 5 de octubre de 2020 a las 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "iot:AttachPrincipalPolicy",
    "iot:AttachThingPrincipal",
    "iot:CreateCertificateFromCsr",
    "iot:CreatePolicy",
    "iot:CreateThing",
    "iot:DescribeCertificate",
    "iot:DescribeThing",
    "iot:DescribeThingGroup",
    "iot:DescribeThingType",
    "iot:DetachPolicy",
    "iot:DetachThingPrincipal",
    "iot:GetPolicy",
    "iot:ListAttachedPolicies",
    "iot:ListPolicyPrincipals",
    "iot:ListPrincipalPolicies",
    "iot:ListPrincipalThings",
    "iot:ListTargetsForPolicy",
    "iot:ListThingGroupsForThing",
    "iot:ListThingPrincipals",
    "iot:RegisterCertificate",
    "iot:RegisterThing",
    "iot:RemoveThingFromThingGroup",
    "iot:UpdateCertificate",
    "iot:UpdateThing",
    "iot:UpdateThingGroupsForThing",
    "iot:AddThingToBillingGroup",
    "iot:DescribeBillingGroup",
    "iot:RemoveThingFromBillingGroup"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTtwinMakerServiceRolePolicy

AWSIoTtwinMakerServiceRolePolicy es una [política AWS gestionada](#) que: permite TwinMaker al AWS IoT llamar a otros AWS servicios y sincronizar sus recursos en tu nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de noviembre de 2023 a las 18:59 UTC
- Hora de edición: 13 de noviembre de 2023 a las 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "iotsitewise:DescribeAsset"
  ],
  "Resource" : [
    "arn:aws:iotsitewise:*:*:asset/*"
  ]
},
{
  "Sid" : "SiteWiseAssetModelReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "iotsitewise:DescribeAssetModel"
  ],
  "Resource" : [
    "arn:aws:iotsitewise:*:*:asset-model/*"
  ]
},
{
  "Sid" : "SiteWiseAssetModelAndAssetListAccess",
  "Effect" : "Allow",
  "Action" : [
    "iotsitewise:ListAssets",
    "iotsitewise:ListAssetModels"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "TwinMakerAccess",
  "Effect" : "Allow",
  "Action" : [
    "iottwinmaker:GetEntity",
    "iottwinmaker:CreateEntity",
    "iottwinmaker:UpdateEntity",
    "iottwinmaker>DeleteEntity",
    "iottwinmaker:ListEntities",
    "iottwinmaker:GetComponentType",
    "iottwinmaker:CreateComponentType",
    "iottwinmaker:UpdateComponentType",
    "iottwinmaker>DeleteComponentType",
    "iottwinmaker:ListComponentTypes"
  ],
  "Resource" : [
    "arn:aws:iottwinmaker:*:*:workspace/*"
  ]
}
```

```
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "iottwinmaker:linkedServices" : [
          "IOTSITWISE"
        ]
      }
    }
  }
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTWirelessDataAccess

AWSIoTWirelessDataAccess es una [política administrada por AWS](#) que: permite el acceso de los datos de identidad asociados a los dispositivos AWS IoT Wireless.

Uso de la política

Puede asociar AWSIoTWirelessDataAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 15:31 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTWirelessFullAccess

AWSIoTWirelessFullAccess es una [política administrada por AWS](#) que: permite que la identidad asociada tenga acceso total a todas las operaciones de AWS IoT Wireless.

Uso de la política

Puede asociar AWSIoTWirelessFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 15:27 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTWirelessFullPublishAccess

AWSIoTWirelessFullPublishAccess es una [política administrada por AWS](#) que: proporciona a IoT Wireless acceso total para publicar en IoT Rules Engine en su nombre.

Uso de la política

Puede asociar AWSIoTWirelessFullPublishAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 15:29 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTWirelessGatewayCertManager

AWSIoTWirelessGatewayCertManager es una [política administrada por AWS](#) que: permite que el acceso a la identidad asociada cree, enumere y describa los certificados de IoT

Uso de la política

Puede asociar AWSIoTWirelessGatewayCertManager a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 15:30 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "IoTWirelessGatewayCertManager",
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateKeysAndCertificate",
      "iot:DescribeCertificate",
      "iot:ListCertificates"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTWirelessLogging

AWSIoTWirelessLogging es una [política administrada por AWS](#) que: permite que la identidad asociada cree grupos de registro de los Registros de Amazon CloudWatch y transmita los registros a los grupos.

Uso de la política

Puede asociar AWSIoTWirelessLogging a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 15:32 UTC

- Hora de edición: 15 de diciembre de 2020 a las 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIoTWirelessReadOnlyAccess

AWSIoTWirelessReadOnlyAccess es una [política administrada por AWS](#) que: permite que la identidad asociada tenga acceso de solo lectura a la tecnología inalámbrica de AWS IoT.

Uso de la política

Puede asociar AWSIoTWirelessReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de diciembre de 2020 a las 15:28 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIPAMServiceRolePolicy

AWSIPAMServiceRolePolicy es una [política administrada por AWS](#) que: permite que el VPC IP Address Manager acceda a los recursos de VPC que se integre con AWS Organizations en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2021 a las 19:08 UTC
- Hora de edición: 08 de noviembre de 2023 a las 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    }
  ]
}
```



```
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIQContractServiceRolePolicy

AWSIQContractServiceRolePolicy es una [política administrada por AWS](#) que: IQ de AWS utiliza para ejecutar solicitudes de pago en nombre de un cliente

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de agosto de 2019 a las 19:28 UTC
- Hora de edición: 22 de agosto de 2019 a las 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIQFullAccess

AWSIQFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a IQ de AWS

Uso de la política

Puede asociar AWSIQFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de abril de 2019 a las 23:13 UTC
- Hora de edición: 25 de septiembre de 2019 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iq:*",
        "iq-permission:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSIQPermissionServiceRolePolicy

AWSIQPermissionServiceRolePolicy es una [política administrada por AWS](#) que: permite que IQ de AWS gestione el rol que asumen los expertos en IQ de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de agosto de 2019 a las 19:36 UTC
- Hora de edición: 22 de agosto de 2019 a las 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteRole",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:AttachRolePolicy"
  ],
  "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
  "Condition" : {
    "ArnEquals" : {
      "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:DetachRolePolicy"
  ],
  "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los servicios y recursos de AWS necesarios para los almacenes de claves personalizadas de AWS KMS

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2018 a las 20:10 UTC
- Hora de edición: 10 de noviembre de 2023 a las 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
      ]
    }
  ],
}
```

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy es una [política administrada AWS](#) que: permite que AWS KMS sincronice las propiedades compartidas de las claves multirregionales.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de junio de 2021 a las 15:37 UTC
- Hora de edición: 16 de junio de 2021 a las 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSKeyManagementServicePowerUser

AWSKeyManagementServicePowerUser es una [política administrada AWS](#) que: proporciona acceso al AWS Key Management Service (KMS).

Uso de la política

Puede asociar AWSKeyManagementServicePowerUser a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 7 de marzo de 2017 a las 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms>DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLakeFormationCrossAccountManager

AWSLakeFormationCrossAccountManager es una [política administrada por AWS](#) que: proporciona acceso entre cuentas a los recursos de Glue a través de Lake Formation. También, otorga acceso de lectura a otros servicios necesarios, como las organizaciones y el administrador de acceso a los recursos

Uso de la política

Puede asociar AWSLakeFormationCrossAccountManager a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de agosto de 2020 a las 20:59 UTC
- Hora de edición: 1 de noviembre de 2023 a las 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLakeFormationDataAdmin

AWSLakeFormationDataAdmin es una [política administrada por AWS](#) que: concede acceso administrativo a Lake Formation y servicios relacionados de AWS, como AWS Glue, para gestionar los lagos de datos

Uso de la política

Puede asociar `AWSLakeFormationDataAdmin` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de agosto de 2019 a las 17:33 UTC
- Hora de edición: 16 de diciembre de 2019 a las 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambda_FullAccess

AWSLambda_FullAccess es una [política administrada por AWS](#) que: otorga acceso total al servicio AWS Lambda, a las características de la consola AWS Lambda y a otros servicios relacionados de AWS.

Uso de la política

Puede asociar AWSLambda_FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de noviembre de 2020 a las 21:14 UTC
- Hora de edición: 17 de noviembre de 2020 a las 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
    "kms:ListAliases",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "lambda:*",
    "logs:DescribeLogGroups",
    "states:DescribeStateMachine",
    "states:ListStateMachines",
    "tag:GetResources",
    "xray:GetTraceSummaries",
    "xray:BatchGetTraces"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:FilterLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}
]
```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambda_ReadOnlyAccess

AWSLambda_ReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura al servicio AWS Lambda, a las características de la consola AWS Lambda y a otros servicios de relacionados de AWS.

Uso de la política

Puede asociar AWSLambda_ReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de noviembre de 2020 a las 21:10 UTC
- Hora de edición: 27 de julio de 2023 a las 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStacks",
      "cloudformation:ListStacks",
      "cloudformation:ListStackResources",
      "cloudwatch:GetMetricData",
      "cloudwatch:ListMetrics",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "kms:ListAliases",
      "iam:GetPolicy",
      "iam:GetPolicyVersion",
      "iam:GetRole",
      "iam:GetRolePolicy",
      "iam:ListAttachedRolePolicies",
      "iam:ListRolePolicies",
      "iam:ListRoles",
      "logs:DescribeLogGroups",
      "lambda:Get*",
      "lambda:List*",
      "states:DescribeStateMachine",
      "states:ListStateMachines",
      "tag:GetResources",
      "xray:GetTraceSummaries",
      "xray:BatchGetTraces"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogStreams",
      "logs:GetLogEvents",
      "logs:FilterLogEvents",
      "logs:StartQuery",
      "logs:StopQuery",
      "logs:DescribeQueries",
      "logs:GetLogGroupFields",
      "logs:GetLogRecord",
      "logs:GetQueryResults"
    ]
  }
]
```

```
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaBasicExecutionRole

AWSLambdaBasicExecutionRole es una [política administrada por AWS](#) que: proporciona permisos de escritura en los Registros de CloudWatch.

Uso de la política

Puede asociar AWSLambdaBasicExecutionRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2015 a las 15:03 UTC
- Hora de edición: 9 de abril de 2015 a las 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaDynamoDBExecutionRole

AWSLambdaDynamoDBExecutionRole es una [política administrada por AWS](#) que: proporciona acceso de lista y lectura a las transmisiones de DynamoDB y permisos de escritura en los registros de CloudWatch.

Uso de la política

Puede asociar AWSLambdaDynamoDBExecutionRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2015 a las 15:09 UTC
- Hora de edición: 9 de abril de 2015 a las 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaENIManagementAccess

AWSLambdaENIManagementAccess es una [política administrada AWS](#) que: proporciona permisos mínimos para que una función de Lambda administre los ENI (crear, describir, eliminar) utilizados por una función Lambda habilitada para VPC.

Uso de la política

Puede asociar AWSLambdaENIManagementAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de diciembre de 2016 a las 00:37 UTC
- Hora de edición: 1 de octubre de 2020 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:AssignPrivateIpAddresses",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaExecute

AWSLambdaExecute es una [política administrada por AWS](#) que: proporciona acceso Put, Get a S3 y acceso total a los Registros de CloudWatch.

Uso de la política

Puede asociar AWSLambdaExecute a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC

- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaFullAccess

AWSLambdaFullAccess es una [política administrada por AWS](#) que: está en vías de caducar. Consulte la documentación para orientarse: <https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html>. Proporciona acceso completo a Lambda, S3, DynamoDB y CloudWatch Metrics y Registros.

Uso de la política

Puede asociar AWSLambdaFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 27 de noviembre de 2017 a las 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"cloudformation:DescribeStackResources",
"cloudformation:DescribeStacks",
"cloudformation:GetTemplate",
"cloudformation:ListStackResources",
"cloudwatch:*",
"cognito-identity:ListIdentityPools",
"cognito-sync:GetCognitoEvents",
"cognito-sync:SetCognitoEvents",
"dynamodb:*",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"events:*",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:ListAttachedRolePolicies",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:PassRole",
"iot:AttachPrincipalPolicy",
"iot:AttachThingPrincipal",
"iot:CreateKeysAndCertificate",
"iot:CreatePolicy",
"iot:CreateThing",
"iot:CreateTopicRule",
"iot:DescribeEndpoint",
"iot:GetTopicRule",
"iot:ListPolicies",
"iot:ListThings",
"iot:ListTopicRules",
"iot:ReplaceTopicRule",
"kinesis:DescribeStream",
"kinesis:ListStreams",
"kinesis:PutRecord",
"kms:ListAliases",
"lambda:*",
"logs:*",
"s3:*",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTopics",
"sns:Publish",
```

```
    "sns:Subscribe",
    "sns:Unsubscribe",
    "sqs:ListQueues",
    "sqs:SendMessage",
    "tag:GetResources",
    "xray:PutTelemetryRecords",
    "xray:PutTraceSegments"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaInvocation-DynamoDB

AWSLambdaInvocation-DynamoDB es una [política administrada por AWS](#) que: proporciona acceso de lectura a DynamoDB Streams.

Uso de la política

Puede asociar AWSLambdaInvocation-DynamoDB a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaKinesisExecutionRole

AWSLambdaKinesisExecutionRole es una [política administrada AWS](#) que: proporciona acceso de lista y lectura a las transmisiones de Kinesis y permisos de escritura en los registros de CloudWatch.

Uso de la política

Puede asociar AWSLambdaKinesisExecutionRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2015 a las 15:14 UTC
- Hora de edición: 19 de noviembre de 2018 a las 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "kinesis:GetRecords",
    "kinesis:GetShardIterator",
    "kinesis:ListShards",
    "kinesis:ListStreams",
    "kinesis:SubscribeToShard",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaMSKExecutionRole

AWSLambdaMSKExecutionRole es una [política administrada por AWS](#) que: proporciona los permisos necesarios para acceder al clúster de MSK dentro de una VPC, administrar los ENI (crear, describir, eliminar) en la VPC y escribir los permisos en los Registros de CloudWatch.

Uso de la política

Puede asociar AWSLambdaMSKExecutionRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de agosto de 2020 a las 17:35 UTC
- Hora de edición: 2 de agosto de 2022 a las 20:08 UTC

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

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:GetBootstrapBrokers",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaReplicator

AWSLambdaReplicator es una [política administrada por AWS](#) que: concede a Lambda Replicator los permisos necesarios para replicar funciones en todas las regiones

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de mayo de 2017 a la 17:53 UTC
- Hora de edición: 8 de diciembre de 2017 a las 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Action" : [
  "lambda:CreateFunction",
  "lambda>DeleteFunction",
  "lambda:DisableReplication"
],
"Resource" : [
  "arn:aws:lambda:*:*:function:*"
]
},
{
  "Sid" : "IamPassRolePermission",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLikeIfExists" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudFrontListDistributions",
  "Effect" : "Allow",
  "Action" : [
    "cloudfront:ListDistributionsByLambdaFunction"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaRole

AWSLambdaRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio de AWS Lambda.

Uso de la política

Puede asociar AWSLambdaRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaSQSQueueExecutionRole

AWSLambdaSQSQueueExecutionRole es una [política administrada por AWS](#) que: proporciona acceso a los atributos de recepción, eliminación de mensajes y lectura a las colas de SQS y permisos de escritura en los registros de CloudWatch.

Uso de la política

Puede asociar AWSLambdaSQSQueueExecutionRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de junio de 2018 a las 21:50 UTC
- Hora de edición: 14 de junio de 2018 a las 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLambdaVPCAccessExecutionRole

AWSLambdaVPCAccessExecutionRole es una [política AWS gestionada](#) que: proporciona permisos mínimos para que una función de Lambda se ejecute mientras se accede a un recurso dentro de una VPC: crear, describir, eliminar interfaces de red y permisos de escritura en los registros. CloudWatch

Uso de la política

Puede asociar `AWSLambdaVPCAccessExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de febrero de 2016 a las 23:15 UTC
- Hora de edición: 5 de enero de 2024 a las 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLicenseManagerConsumptionPolicy

AWSLicenseManagerConsumptionPolicy es una [política administrada por AWS](#) que proporciona permisos para permitir el acceso a las acciones de la API de AWS License Manager necesarias para hacer uso de las licencias a las que el usuario tiene derecho.

Uso de la política

Puede asociar AWSLicenseManagerConsumptionPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de agosto de 2021 a las 23:18 UTC
- Hora de edición: 11 de agosto de 2021 a las 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy es una [política administrada por AWS](#) que: permite a AWS License Manager Linux Subscriptions Service gestionar los recursos en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de diciembre de 2022 a las 18:54 UTC
- Hora de edición: 20 de diciembre de 2022 a las 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
```



```
    "organizations:ListParents",
    "organizations:ListAccountsForParent",
    "organizations:ListRoots",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLicenseManagerMasterAccountRolePolicy

AWSLicenseManagerMasterAccountRolePolicy es una [política administrada por AWS](#) que: es un política de rol de cuenta maestra del servicio de AWS License Manager

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 19:03 UTC
- Hora de edición: 31 de mayo de 2022 a las 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3::aws-license-manager-service-*"
      ]
    }
  ],
  {
```

```
"Sid" : "S3ObjectPermissions2",
"Effect" : "Allow",
"Action" : [
  "s3:DeleteObject"
],
"Resource" : [
  "arn:aws:s3::aws-license-manager-service-*/resource_sync/*"
]
},
{
  "Sid" : "AthenaPermissions",
  "Effect" : "Allow",
  "Action" : [
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:StartQueryExecution"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "GluePermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetTable",
    "glue:GetPartition",
    "glue:GetPartitions"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "OrganizationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "organizations:DescribeAccount",
    "organizations:ListChildren",
    "organizations:ListParents",
    "organizations:ListAccountsForParent",
    "organizations:ListRoots",
```

```
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "RAMPermissions1",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShares",
    "ram:GetResourceShareAssociations",
    "ram:TagResource"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "RAMPermissions2",
  "Effect" : "Allow",
  "Action" : [
    "ram:CreateResourceShare"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Service" : "LicenseManager"
    }
  }
},
{
  "Sid" : "RAMPermissions3",
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceShare",
    "ram:DisassociateResourceShare",
    "ram:UpdateResourceShare",
    "ram>DeleteResourceShare"
  ],
  "Resource" : [
    "*"
  ]
}
```

```
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/Service" : "LicenseManager"
      }
    }
  },
  {
    "Sid" : "IAMGetRoles",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "IAMPassRoles",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "cloudformation.amazonaws.com",
          "glue.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "CloudformationPermission",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:UpdateStack",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks"
    ]
  },
  ],
```

```

    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/
LicenseManagerCrossAccountCloudDiscoveryStack/*"
    ]
  },
  {
    "Sid" : "GlueUpdatePermissions",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateTable",
      "glue:UpdateTable",
      "glue>DeleteTable",
      "glue:UpdateJob",
      "glue:UpdateCrawler"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler",
      "arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob",
      "arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*",
      "arn:aws:glue:*:*:table/license_manager_resource_sync/*",
      "arn:aws:glue:*:*:database/license_manager_resource_inventory_db",
      "arn:aws:glue:*:*:database/license_manager_resource_sync"
    ]
  },
  {
    "Sid" : "RGPermissions",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:PutGroupPolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "ram.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLicenseManagerMemberAccountRolePolicy

AWSLicenseManagerMemberAccountRolePolicy es una [política administrada por AWS](#) que: es una política de rol de cuenta de miembro del servicio de AWS License Manager

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 19:04 UTC
- Hora de edición: 15 de noviembre de 2019 a las 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Sid" : "LicenseManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "license-manager:UpdateLicenseSpecificationsForResource",
      "license-manager:GetLicenseConfiguration"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "SSMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListInventoryEntries",
      "ssm:GetInventory",
      "ssm:CreateAssociation",
      "ssm:CreateResourceDataSync",
      "ssm>DeleteResourceDataSync",
      "ssm:ListResourceDataSync",
      "ssm:ListAssociations"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "RAMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ram:AcceptResourceShareInvitation",
      "ram:GetResourceShareInvitations"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLicenseManagerServiceRolePolicy

AWSLicenseManagerServiceRolePolicy es una [política administrada AWS](#) que: es una política de rol predeterminado del servicio de AWS License Manager

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 19:02 UTC
- Hora de edición: 30 de julio de 2021 a las 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
    }
  }
},
{
  "Sid" : "IAMPermissionsForCreatingMemberSLR",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
    }
  }
},
{
  "Sid" : "S3BucketPermissions1",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-license-manager-service-*"
  ]
},
{
  "Sid" : "S3BucketPermissions2",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "S3ObjectPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-license-manager-service-*"
    ]
  },
  {
    "Sid" : "SNSAccountPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : [
      "arn:aws:sns:*:*:aws-license-manager-service-*"
    ]
  },
  {
    "Sid" : "SNSTopicPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "EC2Permissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeHosts"
    ],
    "Resource" : [
```

```
        "*"
    ]
},
{
    "Sid" : "SSMPermissions",
    "Effect" : "Allow",
    "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "OrganizationPermissions",
    "Effect" : "Allow",
    "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "LicenseManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

AWSLicenseManagerUserSubscriptionsServiceRolePolicy es una [política administrada por AWS](#) que: permite que el Servicio de Suscripciones de Usuarios de AWS License Manager gestione los recursos en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de julio de 2022 a las 01:17 UTC
- Hora de edición: 21 de noviembre de 2022 a las 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Sid" : "DSReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ds:DescribeDirectories",
      "ds:GetAuthorizedApplicationDetails"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SSMReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetInventory",
      "ssm:GetCommandInvocation",
      "ssm:ListCommandInvocations",
      "ssm:DescribeInstanceInformation"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2ReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeVpcPeeringConnections"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2WritePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:CreateTags"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:productCode" : [
          "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"
    }
  }
}
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSM2ServicePolicy

AWSM2ServicePolicy es una [política administrada por AWS](#) que: permite que AWS M2 gestione los recursos de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de junio de 2022 a las 20:26 UTC
- Hora de edición: 7 de junio de 2022 a las 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ]
    }
  ],
}
```



```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:DeregisterTargets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/M2"
        ]
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSManagedServices_ContactsServiceRolePolicy

AWSManagedServices_ContactsServiceRolePolicy es una [política administrada por AWS](#) que: permite que Managed Services AWS lea los valores de las etiquetas de los recursos de AWS

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de marzo de 2023 a las 17:07 UTC
- Hora de edición: 23 de marzo de 2023 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoleTags",
      "iam:ListUserTags",
      "tag:GetResources",
      "ec2:DescribeTags"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "s3:GetBucketTagging",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "s3:authType" : "REST-HEADER",
        "s3:signatureversion" : "AWS4-HMAC-SHA256"
      },
      "NumericGreaterThanEquals" : {
        "s3:TlsVersion" : "1.2"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy es una [política administrada por AWS](#) que: usa Managed Services de AWS para gestionar la infraestructura de controles de detección

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de diciembre de 2022 a las 23:11 UTC
- Hora de edición: 19 de diciembre de 2022 a las 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateTermination*",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
```

```

    "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-recorder",
    "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-rules-cdk",
    "arn:aws:cloudformation:*:*:stack/ams-detective-controls-infrastructure-cdk"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeAggregationAuthorizations",
    "config:PutAggregationAuthorization",
    "config:TagResource",
    "config:PutConfigRule"
  ],
  "Resource" : [
    "arn:aws:config:*:*:aggregation-authorization/540708452589/*",
    "arn:aws:config:*:*:config-rule/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketPolicy",
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3>DeleteBucketPolicy",
    "s3>DeleteObject",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:GetBucketAcl",
    "s3:PutObject",
    "s3:PutBucketAcl",
    "s3:PutBucketLogging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketTagging",
    "s3:PutBucketVersioning",
    "s3:PutEncryptionConfiguration"
  ],
  "Resource" : "arn:aws:s3:::ams-config-record-bucket-*"
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSManagedServices_EventsServiceRolePolicy

AWSManagedServices_EventsServiceRolePolicy es una [política administrada por AWS](#) que: usa Managed Services de AWS para habilitar la característica de procesador de eventos AMS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de febrero de 2023 a las 18:41 UTC
- Hora de edición: 7 de febrero de 2023 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "events:DeleteRule",
  "events:PutTargets",
  "events:PutRule",
  "events:RemoveTargets"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "events:ManagedBy" : "events.managedservices.amazonaws.com"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSManagedServicesDeploymentToolkitPolicy

AWSManagedServicesDeploymentToolkitPolicy es una [política administrada por AWS](#) que: permite que AWSManaged Services gestione el kit de herramientas de implementación en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de junio de 2022 a las 18:33 UTC
- Hora de edición: 10 de mayo de 2023 a las 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceAmiIngestion

AWSMarketplaceAmiIngestion es una [política administrada por AWS](#) que: permite que AWS Marketplace copie las imágenes de máquina de Amazon (AMI) para incluirlas en AWS Marketplace

Uso de la política

Puede asociar AWSMarketplaceAmiIngestion a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de septiembre de 2020 a las 20:55 UTC
- Hora de edición: 25 de septiembre de 2020 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
    },
    {
      "Action" : [
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceDeploymentServiceRolePolicy

AWSMarketplaceDeploymentServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Marketplace cree y gestione los parámetros de implementación del vendedor para los productos a los que se suscribe en AWS Marketplace.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2023 a las 23:34 UTC
- Hora de edición: 15 de noviembre de 2023 a las 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

"Action" : [
  "secretsmanager:CreateSecret",
  "secretsmanager:PutSecretValue",
  "secretsmanager:DescribeSecret",
  "secretsmanager>DeleteSecret",
  "secretsmanager:RemoveRegionsFromReplication"
],
"Resource" : [
  "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "ListSecrets",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:ListSecrets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "TagMarketplaceDeploymentSecrets",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/expirationDate" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "expirationDate"
      ]
    }
  },
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}

```

```
}  
  }  
    }  
  ]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceFullAccess

AWSMarketplaceFullAccess es una [política administrada por AWS](#) que: ofrece la posibilidad de realizar y cancelar suscripciones a software de AWS Marketplace. Permite que los usuarios administren instancias de software de Marketplace desde la página 'Your Software' de Marketplace y proporciona acceso administrativo a EC2.

Uso de la política

Puede asociar AWSMarketplaceFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de febrero de 2015 a las 17:21 UTC
- Hora de edición: 4 de marzo de 2022 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2>DeleteSnapshot",

```

```

    "ec2:CreateImage",
    "ec2:DescribeInstanceStatus",
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:DescribeDocument",
    "sns:ListTopics",
    "sns:GetTopicAttributes",
    "sns:CreateTopic",
    "iam:GetRole",
    "iam:GetInstanceProfile",
    "iam:ListRoles",
    "iam:ListInstanceProfiles"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "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/*"
        ]
      }
    }
  }
}
```

```
}  
  }  
    }  
  ]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceGetEntitlements

AWSMarketplaceGetEntitlements es una [política administrada por AWS](#) que: proporciona acceso de lectura a los Derechos de AWS Marketplace

Uso de la política

Puede asociar AWSMarketplaceGetEntitlements a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de marzo de 2017 a las 19:37 UTC
- Hora de edición: 27 de marzo de 2017 a las 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceImageBuildFullAccess

AWSMarketplaceImageBuildFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a la característica de creación de imágenes privadas de AWS Marketplace. Además de crear imágenes privadas, también concede permisos para añadir etiquetas a las imágenes, y lanzar y finalizar instancias ec2.

Uso de la política

Puede asociar AWSMarketplaceImageBuildFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 31 de julio de 2018 a las 23:29 UTC
- Hora de edición: 4 de marzo de 2022 a las 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:StartBuild",
        "aws-marketplace:DescribeBuilds"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
        }
      }
    }
  ],
  {
```

```

    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/*Automation*",
      "arn:aws:iam::*:role/*Instance*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution",
      "ssm:ListDocuments",
      "ssm:DescribeDocument",
      "ec2:DeregisterImage",
      "ec2:CopyImage",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeImages",
      "ec2:DescribeSubnets",
      "ec2>DeleteSnapshot",
      "ec2:CreateImage",
      "ec2:RunInstances",
      "ec2:DescribeInstanceStatus",
      "sns:GetTopicAttributes",
      "iam:GetRole",
      "iam:GetInstanceProfile"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3::*:image-build*"
    ]
  }
}

```

```

    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : [
      "arn:aws:sns:*:*:*image-build*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartAutomationExecution"
    ],
    "Resource" : [
      "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
      "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
      "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
      "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
      "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
      "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
      "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
      "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "*"
    ]
  }

```

```

    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "ssm.amazonaws.com"
        ],
        "iam:AssociatedResourceARN" : [
          "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
          "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
          "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
          "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
          "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
          "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
          "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
          "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
        ]
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/marketplace-image-build:build-id" : "*"
      },
      "StringNotEquals" : {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

AWSMarketplaceLicenseManagementServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los recursos de Servicios de AWS utilizados o gestionados por AWS Marketplace para la administración de licencias.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2020 a las 08:33 UTC
- Hora de edición: 3 de diciembre de 2020 a las 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
"Statement" : [
  {
    "Sid" : "AllowLicenseManagerActions",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeOrganization",
      "license-manager:ListReceivedGrants",
      "license-manager:ListDistributedGrants",
      "license-manager:GetGrant",
      "license-manager:CreateGrant",
      "license-manager:CreateGrantVersion",
      "license-manager>DeleteGrant",
      "license-manager:AcceptGrant"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions es una [política administrada por AWS](#) que: ofrece la posibilidad de suscribirse y cancelar la suscripción al software de AWS Marketplace

Uso de la política

Puede asociar AWSMarketplaceManageSubscriptions a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC

- Hora de edición: 19 de enero de 2023 a las 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceMeteringFullAccess

AWSMarketplaceMeteringFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a AWS Marketplace Metering.

Uso de la política

Puede asociar AWSMarketplaceMeteringFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de marzo de 2016 a las 22:39 UTC
- Hora de edición: 17 de marzo de 2016 a las 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceMeteringRegisterUsage

AWSMarketplaceMeteringRegisterUsage es una [política administrada por AWS](#) que: proporciona permisos para registrar un recurso y realizar un seguimiento del uso a través de AWS Marketplace Metering Service.

Uso de la política

Puede asociar AWSMarketplaceMeteringRegisterUsage a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 21 de noviembre de 2019 a las 01:17 UTC
- Hora de edición: 21 de noviembre de 2019 a las 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceProcurementSystemAdminFullAccess

AWSMarketplaceProcurementSystemAdminFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a todas las acciones administrativas para la integración de la contratación electrónica de AWS Marketplace.

Uso de la política

Puede asociar AWSMarketplaceProcurementSystemAdminFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de junio de 2019 a las 13:07 UTC
- Hora de edición: 25 de junio de 2019 a las 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
```

```
    "organizations:Describe*",
    "organizations:List*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

AWSMarketplacePurchaseOrdersServiceRolePolicy es una [política administrada por AWS](#) que: permite que los servicios de AWS Marketplace accedan a la gestión de pedidos de compra.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de octubre de 2021 a las 15:12 UTC
- Hora de edición: 27 de octubre de 2021 a las 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceRead-only

AWSMarketplaceRead-only es una [política administrada por AWS](#) que: ofrece la posibilidad de revisar las suscripciones de AWS Marketplace

Uso de la política

Puede asociar `AWSMarketplaceRead-only` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 19 de enero de 2023 a las 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

AWSMarketplaceResaleAuthorizationServiceRolePolicy es una [política AWS gestionada](#) que: permite el acceso a Servicios de AWS los recursos utilizados o gestionados por ellos AWS Marketplace para la autorización de reventa.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de marzo de 2024 a las 18:47 UTC
- Hora editada: 5 de marzo de 2024 a las 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
```

```

    "arn:aws:ram:*:*:*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ram:RequestedResourceType" : "aws-marketplace:Entity"
    },
    "ArnLike" : {
      "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/
ResaleAuthorization/*"
    },
    "Null" : {
      "ram:Principal" : "true"
    }
  }
},
{
  "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceShare"
  ],
  "Resource" : [
    "arn:aws:ram:*:*:*"
  ],
  "Condition" : {
    "Null" : {
      "ram:Principal" : "false"
    },
    "StringEquals" : {
      "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
    }
  }
},
{
  "Sid" : "AllowResaleAuthorizationShareActionsRAMAccept",
  "Effect" : "Allow",
  "Action" : [
    "ram:AcceptResourceShareInvitation"
  ],
  "Resource" : [
    "arn:aws:ram:*:*:*"
  ],
  "Condition" : {
    "StringEquals" : {

```

```
        "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
    }
}
},
{
    "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
    "Effect" : "Allow",
    "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
    ],
    "Resource" : [
        "arn:aws:ram:*:*:*"
    ]
},
{
    "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
    "Effect" : "Allow",
    "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy"
    ],
    "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "ram.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
    "Effect" : "Allow",
    "Action" : [
        "aws-marketplace:DescribeEntity"
    ],
    "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
}
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSMarketplaceSellerFullAccess

AWSMarketplaceSellerFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a todas las operaciones de los vendedores en el AWS Marketplace y otros AWS servicios, como la gestión de la AMI.

Uso de la política

Puede asociar AWSMarketplaceSellerFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de julio de 2019 a las 20:40 UTC
- Hora editada: 15 de marzo de 2024 a las 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSMarketplaceSellerProductsFullAccess

AWSMarketplaceSellerProductsFullAccess es una [política administrada por AWS](#) que concede a los vendedores acceso total a la página de Productos de gestión de AWS Marketplace y a otros servicios de AWS, como la gestión de AMI.

Uso de la política

Puede asociar AWSMarketplaceSellerProductsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de julio de 2019 a las 21:06 UTC
- Hora de edición: 18 de julio de 2023 a las 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace: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/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMarketplaceSellerProductsReadOnly

AWSMarketplaceSellerProductsReadOnly es una [política administrada por AWS](#) que: otorga a los vendedores acceso de solo lectura a la página de Productos de gestión de AWS Marketplace.

Uso de la política

Puede asociar AWSMarketplaceSellerProductsReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de julio de 2019 a las 21:40 UTC
- Hora de edición: 19 de noviembre de 2022 a las 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMediaConnectServicePolicy

AWSMediaConnectServicePolicy es una [política administrada por AWS](#) que: es una política predeterminada que permite el acceso a Servicios de AWS y los recursos utilizados o gestionados por MediaConnect.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de abril de 2023 a las 22:11 UTC
- Hora de edición: 3 de abril de 2023 a las 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs>DeleteService",
        "ecs>CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs>DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
```

```

    "ecs:StopTask",
    "ecs:DescribeTasks",
    "ecs:DescribeContainerInstances",
    "ecs:UpdateContainerInstancesState"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:RegisterTaskDefinition"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateCluster",
    "ecs:UpdateClusterSettings",
    "ecs:ListAttributes",
    "ecs:DescribeClusters",
    "ecs:DeregisterContainerInstance",
    "ecs:ListContainerInstances"
  ],
  "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMediaTailorServiceRolePolicy

AWSMediaTailorServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los recursos de AWS utilizados o gestionados por MediaTailor

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de septiembre de 2021 a las 22:27 UTC
- Hora de edición: 17 de septiembre de 2021 a las 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubDiscoveryAccess

AWSMigrationHubDiscoveryAccess es una [política administrada por AWS](#) que: permite que AWSMigrationHubService llame a AWSApplicationDiscoveryService en nombre del cliente.

Uso de la política

Puede asociar AWSMigrationHubDiscoveryAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 13:30 UTC
- Hora de edición: 6 de agosto de 2020 a las 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstanceAttribute"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubDMSAccess

AWSMigrationHubDMSAccess es una [política administrada por AWS](#) que: sirve para que Database Migration Service asuma un rol en la cuenta del cliente para llamar a Migration Hub

Uso de la política

Puede asociar AWSMigrationHubDMSAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 14:00 UTC
- Hora de edición: 7 de octubre de 2019 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh>ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh>ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
    },
    {
      "Action" : [
        "mgh>ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
    }
  ]
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubFullAccess

AWSMigrationHubFullAccess es una [política administrada por AWS](#) que: brinda al cliente acceso al servicio Migration Hub

Uso de la política

Puede asociar AWSMigrationHubFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de agosto de 2017 a las 14:02 UTC
- Hora de edición: 19 de junio de 2019 a las 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
    }
  ]
}
```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "migrationhub.amazonaws.com",
          "dmsintegration.migrationhub.amazonaws.com",
          "smsintegration.migrationhub.amazonaws.com"
        ]
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubOrchestratorConsoleFullAccess

AWSMigrationHubOrchestratorConsoleFullAccess es una [política administrada de AWS](#) que concede acceso limitado a AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service y AWS Secrets Manager. Esta política también concede acceso completo al servicio Orquestador de AWS Migration Hub.

Uso de la política

Puede asociar `AWSMigrationHubOrchestratorConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de abril de 2022 a las 02:26 UTC
- Hora editada: 5 de diciembre de 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

AWSMigrationHubOrchestratorInstanceRolePolicy es una [política administrada por AWS](#) que: debe asociarse a las instancias migradas de SAP y MGN para que nuestro servicio pueda organizarlas mediante la descarga de scripts de S3 y obtener valores secretos dentro de la instancia de EC2.

Uso de la política

Puede asociar `AWSMigrationHubOrchestratorInstanceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de abril de 2022 a las 02:43 UTC
- Hora de edición: 20 de abril de 2022 a las 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3::migrationhub-orchestrator-*",
        "arn:aws:s3::aws-migrationhub-orchestrator-*/*"
    ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubOrchestratorPlugin

AWSMigrationHubOrchestratorPlugin es una [política administrada por AWS](#) que: concede acceso limitado a Simple Storage Service de Amazon, AWSSecrets Manager y acciones relacionadas con complementos para AWS Migration Hub Orchestrator.

Uso de la política

Puede asociar AWSMigrationHubOrchestratorPlugin a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de abril de 2022 a las 02:25 UTC
- Hora de edición: 20 de abril de 2022 a las 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/*prod/*/*put-log-data",
        "arn:aws:execute-api:*:*:*/*prod/*/*put-metric-data"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:RegisterPlugin",
        "migrationhub-orchestrator:GetMessage",
        "migrationhub-orchestrator:SendMessage"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubOrchestratorServiceRolePolicy

AWSMigrationHubOrchestratorServiceRolePolicy es una [política administrada de AWS](#) que proporciona los permisos necesarios para que el Orquestador de Migration Hub migre y modernice las cargas de trabajo en las instalaciones

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de abril de 2022 a las 02:24 UTC
- Hora editada: 4 de marzo de 2024 a las 18:25 UTC

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

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
    }
  ]
}
```

```

    "Resource" : "*"
  },
  {
    "Sid" : "ec2MGNLaunchTemplate",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ec2LaunchTemplates",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeLaunchTemplates"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "getHomeRegion",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "SSMcommand",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand",
      "ssm:GetCommandInvocation",
      "ssm:CancelCommand"
    ],
    "Resource" : [
      "arn:aws:ssm:*::document/AWS-RunRemoteScript",
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:s3:::aws-migrationhub-orchestrator-*",

```

```

    "arn:aws:s3::migrationhub-orchestrator-*"
  ]
},
{
  "Sid" : "SSM",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeInstanceInformation",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "s3GetObject",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::migrationhub-orchestrator-*",
    "arn:aws:s3::migrationhub-orchestrator-*/*"
  ]
},
{
  "Sid" : "EventBridge",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:DescribeRule",
    "events>DeleteRule",
    "events:PutRule",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
},
{
  "Sid" : "MGN",
  "Effect" : "Allow",
  "Action" : [
    "mgn:GetReplicationConfiguration",
    "mgn:GetLaunchConfiguration",
    "mgn:StartCutover",

```

```
    "mgn:FinalizeCutover",
    "mgn:StartTest",
    "mgn:UpdateReplicationConfiguration",
    "mgn:DescribeSourceServers",
    "mgn:MarkAsArchived",
    "mgn:ChangeServerLifeCycleState"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ec2DescribeImportImage",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeImportImageTasks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "s3ListBucket",
  "Effect" : "Allow",
  "Action" : "s3:ListBucket",
  "Resource" : "arn:aws:s3:::*",
  "Condition" : {
    "StringLike" : {
      "s3:prefix" : "migrationhub-orchestrator-vmie-*"
    }
  }
}
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSMigrationHubRefactorSpaces- EnvironmentsWithoutBridgesFullAccess

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess es una [política administrada por AWS](#) que: otorga acceso total a AWS Migration Hub Refactor Spaces y otros servicios de AWS relacionados, excepto la Puerta de enlace de AWS Transit y los grupos de seguridad de EC2, que no son necesarios cuando se utilizan entornos sin un puente de red. Esta política también excluye los permisos necesarios para AWS Lambda y AWS Resource Access Manager, ya que su alcance se puede reducir según las etiquetas.

Uso de la política

Puede asociar AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de abril de 2023 a las 20:09 UTC
- Hora de edición: 20 de julio de 2023 a las 15:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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-
n1b-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateListener"
    ],
    "Resource" : [
      "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-n1b-*",
      "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-n1b-*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing>DeleteListener",
  "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-n1b-*"
},
{
  "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"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy es una [política administrada por AWS](#) que se utiliza en el rol de servicio de IAM transferido al documento de automatización de SSM AWSRefactorSpaces-CreateResources para conceder los permisos necesarios para ejecutar la automatización. La política otorga acceso de lectura y escritura a las etiquetas de EC2, para realizar un seguimiento del progreso de la automatización. Cuando se habilita el puente de red del entorno de Refactor Spaces, la automatización también agrega el grupo de seguridad del entorno a la instancia de EC2, para permitir el tráfico desde otros servicios de Refactor Spaces del entorno. A su vez, la política permite el acceso a los parámetros SSM de las acciones posteriores al lanzamiento del Servicio de migración de aplicaciones.

Uso de la política

Puede asociar AWSMigrationHubRefactorSpaces-SSMAutomationPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de agosto de 2023 a las 15:08 UTC
- Hora de edición: 10 de agosto de 2023 a las 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstances"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyInstanceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyInstanceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
    }
  }
},
{
```

```
    "Effect" : "Allow",
    "Action" : "ssm:GetParameters",
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubRefactorSpacesFullAccess

AWSMigrationHubRefactorSpacesFullAccess es una [política administrada por AWS](#) que: otorga acceso completo a AWS MigrationHub Refactor Spaces, a las características de la consola de AWS MigrationHub Refactor Spaces y a otros servicios de AWS relacionados, excepto los permisos necesarios para AWS Lambda y AWS Resource Access Manager, ya que se pueden determinar en función de las etiquetas.

Uso de la política

Puede asociar AWSMigrationHubRefactorSpacesFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2021 a las 07:12 UTC
- Hora de edición: 19 de julio de 2023 a las 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

AWSMigrationHubRefactorSpacesServiceRolePolicy es una [política administrada por AWS](#) que: concede acceso a los recursos AWS gestionados o utilizados por AWS Migration Hub Refactor Spaces.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2021 a las 06:50 UTC
- Hora de edición: 20 de julio de 2023 a las 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2>DeleteRoute",
        "ec2>DeleteTags",
        "ram>DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    }
  ],
  {
```

```

    "Effect" : "Allow",
    "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:CreateLoadBalancerListeners",
      "elasticloadbalancing:CreateListener",
      "elasticloadbalancing>DeleteListener",
      "elasticloadbalancing>DeleteTargetGroup"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/refactor-spaces:route-id" : [
          "*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:PUT",
      "apigateway:POST",
      "apigateway:GET",
      "apigateway:PATCH",
      "apigateway:DELETE"
    ],
    "Resource" : [
      "arn:aws:apigateway:*::/restapis",
      "arn:aws:apigateway:*::/restapis/*",
      "arn:aws:apigateway:*::/vpclinks/*",
      "arn:aws:apigateway:*::/tags",
      "arn:aws:apigateway:*::/tags/*"
    ],
    "Condition" : {

```

```
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "apigateway:GET",
    "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DeleteLoadBalancer",
    "Resource" : "arn:*:elasticloadbalancing:*::loadbalancer/net/refactor-spaces-
nlb-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateListener"
    ],
    "Resource" : [
      "arn:*:elasticloadbalancing:*::loadbalancer/net/refactor-spaces-nlb-*",
      "arn:*:elasticloadbalancing:*::listener/net/refactor-spaces-nlb-*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing>DeleteListener",
    "Resource" : "arn:*:elasticloadbalancing:*::listener/net/refactor-spaces-nlb-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing>DeleteTargetGroup",
      "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*::targetgroup/refactor-spaces-tg-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubSMSAccess

AWSMigrationHubSMSAccess es una [política administrada por AWS](#) que: se otorga para que el Servicio de Migración de Servidores asuma un rol en la cuenta del cliente para llamar a Migration Hub

Uso de la política

Puede asociar `AWSMigrationHubSMSAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 13:57 UTC
- Hora de edición: 7 de octubre de 2019 a las 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh>ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
```

```
    "mgh:PutResourceAttributes",
    "mgh:NotifyApplicationState",
    "mgh:DescribeApplicationState",
    "mgh:AssociateDiscoveredResource",
    "mgh:DisassociateDiscoveredResource",
    "mgh:ListDiscoveredResources"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
},
{
  "Action" : [
    "mgh:ListMigrationTasks",
    "mgh:GetHomeRegion"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubStrategyCollector

AWSMigrationHubStrategyCollector es una [política administrada por AWS](#) que: concede permisos para permitir la comunicación con el servicio de AWSMigration Hub Strategy Recommendations, el acceso de lectura y escritura a los buckets de S3 relacionados con el servicio, el acceso a Amazon API Gateway para cargar registros y métricas a AWS, el acceso de AWS Secrets Manager para recuperar credenciales y cualquier servicio relacionado.

Uso de la política

Puede asociar `AWSMigrationHubStrategyCollector` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de octubre de 2021 a las 20:15 UTC
- Hora editada: 5 de febrero de 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "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}"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubStrategyConsoleFullAccess

AWSMigrationHubStrategyConsoleFullAccess es una [política administrada por AWS](#) que otorga acceso completo al servicio de recomendaciones estratégicas de AWS Migration Hub y acceso a los servicios de AWS relacionados a través de la AWS Management Console.

Uso de la política

Puede asociar `AWSMigrationHubStrategyConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de octubre de 2021 a las 20:13 UTC
- Hora de edición: 9 de noviembre de 2022 a las 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "s3:GetObject",
      "s3:CreateBucket",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketPolicy",
      "s3:PutBucketVersioning",
      "s3:PutLifecycleConfiguration"
    ],
    "Resource" : "arn:aws:s3::migrationhub-strategy-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:ListSecrets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "discovery:GetDiscoverySummary",
      "discovery:DescribeTags",
      "discovery:DescribeConfigurations",
      "discovery:ListConfigurations"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ]
  }

```

```
    ],  
    "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-  
strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"  
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMigrationHubStrategyServiceRolePolicy

AWSMigrationHubStrategyServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los recursos de AWS utilizados o gestionados por el servicio de recomendaciones estratégicas de AWS Migration Hub.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de octubre de 2021 a las 20:02 UTC
- Hora de edición: 19 de octubre de 2021 a las 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "permissionsForAds",
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "permissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    }
  ]
}
```

```
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMobileHub_FullAccess

AWSMobileHub_FullAccess es una [política administrada por AWS](#) que: se puede asociar a cualquier usuario, rol o grupo para conceder a los usuarios permiso para crear, eliminar y modificar proyectos (y los recursos de AWS asociados) en Mobile Hub de AWS. También, incluye permisos para generar y descargar ejemplos de código fuente de aplicaciones móviles, para cada proyecto de Mobile Hub.

Uso de la política

Puede asociar AWSMobileHub_FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de enero de 2016 a las 19:56 UTC
- Hora de edición: 19 de diciembre de 2019 a las 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
    }
  ]
}
```

```
    "Resource" : "arn:aws:s3::*/aws-my-sample-app*.zip"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject"
    ],
    "Resource" : "arn:aws:s3::*-mobilehub-*/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket"
    ],
    "Resource" : "arn:aws:s3::*-mobilehub-*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMobileHub_ReadOnly

AWSMobileHub_ReadOnly es una [política administrada por AWS](#) que: se puede asociar a cualquier usuario, rol o grupo para conceder a los usuarios permiso para publicar y ver proyectos en Mobile Hub de AWS. También, incluye permisos para generar y descargar ejemplos de código fuente de aplicaciones móviles, para cada proyecto de Mobile Hub. No permite al usuario modificar configuraciones de los proyectos de Mobile Hub.

Uso de la política

Puede asociar AWSMobileHub_ReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 5 de enero de 2016 a las 19:55 UTC
- Hora de edición: 23 de julio de 2018 a las 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:ExportProject",
        "mobilehub:GenerateProjectParameters",
        "mobilehub:GetProject",
        "mobilehub:SynchronizeProject",
        "mobilehub:GetProjectSnapshot",
      ]
    }
  ]
}
```

```

    "mobilehub:ListProjectSnapshots",
    "mobilehub:ListAvailableConnectors",
    "mobilehub:ListAvailableFeatures",
    "mobilehub:ListAvailableRegions",
    "mobilehub:ListProjects",
    "mobilehub:ValidateProject",
    "mobilehub:VerifyServiceRole",
    "mobilehub:DescribeBundle",
    "mobilehub:ExportBundle",
    "mobilehub:ListBundles"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "arn:aws:s3::*/aws-my-sample-app*.zip"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSMSKReplicatorExecutionRole

AWSMSKReplicatorExecutionRole es una [política AWS gestionada](#) que: concede permisos a Amazon MSK Replicator para replicar datos entre clústeres de MSK.

Uso de la política

Puede asociar AWSMSKReplicatorExecutionRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de diciembre de 2023 a las 00:07 UTC
- Hora editada: 6 de diciembre de 2023, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration"
      ],
      "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/*/*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSNetworkFirewallServiceRolePolicy

AWSNetworkFirewallServiceRolePolicy es una [política administrada AWS](#) que: permite que AWSNetworkFirewall cree y administre los recursos necesarios para los firewalls.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2020 a las 17:17 UTC
- Hora de edición: 30 de marzo de 2023 a las 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ]
    }
  ]
}
```

```
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "acm:DescribeCertificate",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "resource-groups:ListGroupResources",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "tag:GetResources",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "resource-groups.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint",
        "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "*",
    "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSNetworkManagerCloudWANServiceRolePolicy

AWSNetworkManagerCloudWANServiceRolePolicy es una [política administrada por AWS](#) que: permite que NetworkManager acceda a los recursos asociados a su red principal

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de julio de 2022 a las 12:17 UTC
- Hora de edición: 12 de julio de 2022 a las 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2>DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSNetworkManagerFullAccess

`AWSNetworkManagerFullAccess` es una [política administrada por AWS](#) que: brinda acceso completo a Amazon NetworkManager a través de la AWS Management Console.

Uso de la política

Puede asociar `AWSNetworkManagerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 3 de diciembre de 2019 a las 17:37 UTC
- Hora de edición: 3 de diciembre de 2019 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSNetworkManagerReadOnlyAccess

`AWSNetworkManagerReadOnlyAccess` es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Amazon NetworkManager a través de la AWS Management Console.

Uso de la política

Puede asociar `AWSNetworkManagerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de diciembre de 2019 a las 17:35 UTC
- Hora de edición: 3 de diciembre de 2019 a las 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSNetworkManagerServiceRolePolicy

AWSNetworkManagerServiceRolePolicy es una [política administrada por AWS](#) que: permite que NetworkManager accede a los recursos asociados a sus Redes globales

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2019 a las 14:03 UTC
- Hora de edición: 27 de julio de 2022 a las 19:41 UTC

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

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeLocations",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpcs",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeRegions",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",

```



```
    "ec2:DescribeTransitGatewayRouteTableAnnouncements",
    "ec2:DescribeTransitGatewayPolicyTables",
    "ec2:GetTransitGatewayPolicyTableAssociations",
    "ec2:GetTransitGatewayPolicyTableEntries"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOpsWorks_FullAccess

AWSOpsWorks_FullAccess es una [política administrada por AWS](#) que: brinda acceso total a OpsWorks de AWS.

Uso de la política

Puede asociar AWSOpsWorks_FullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de enero de 2021 a las 16:29 UTC
- Hora de edición: 22 de enero de 2021 a las 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "iam:ListUsers",
        "opsworks:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "opsworks.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOpsWorksCloudWatchLogs

AWSOpsWorksCloudWatchLogs es una [política administrada por AWS](#) que: permite que las instancias de OpsWorks junto con la integración de CWLogs habilitada envíen registros y creen los grupos de registros necesarios

Uso de la política

Puede asociar AWSOpsWorksCloudWatchLogs a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de marzo de 2017 a las 17:47 UTC
- Hora de edición: 30 de marzo de 2017 a las 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOpsWorksCMInstanceProfileRole

AWSOpsWorksCMInstanceProfileRole es una [política administrada por AWS](#) que: proporciona acceso a S3 para las instancias lanzadas por OpsWorks CM.

Uso de la política

Puede asociar AWSOpsWorksCMInstanceProfileRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de noviembre de 2016 a las 09:48 UTC
- Hora de edición: 23 de abril de 2021 a las 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:SignalResource"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
    },
  ]
}
```

```
    "Resource" : "arn:aws:s3:::aws-opsworks-cm-*",
    "Effect" : "Allow"
  },
  {
    "Action" : "acm:GetCertificate",
    "Resource" : "*",
    "Effect" : "Allow"
  },
  {
    "Action" : "secretsmanager:GetSecretValue",
    "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
    "Effect" : "Allow"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOpsWorksCMServiceRole

AWSOpsWorksCMServiceRole es una [política administrada por AWS](#) que: es una Política de roles de servicio que se utiliza para crear servidores CM de OpsWorks.

Uso de la política

Puede asociar AWSOpsWorksCMServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de noviembre de 2016 a las 09:49 UTC
- Hora de edición: 23 de abril de 2021 a las 17:32 UTC

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

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:GetBucketTagging",
        "s3:PutBucketTagging"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "tag:UntagResources",
        "tag:TagResources"
      ]
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Action" : [
    "ssm:DescribeInstanceInformation",
    "ssm:GetCommandInvocation",
    "ssm:ListCommandInvocations",
    "ssm:ListCommands"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
    }
  },
  "Action" : [
    "ssm:SendCommand"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:ssm:*::document/*",
    "arn:aws:s3:::aws-opsworks-cm-*"
  ],
  "Action" : [
    "ssm:SendCommand"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AssociateAddress",
```



```

    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateImage",
    "ec2:CreateSecurityGroup",
    "ec2:CreateSnapshot",
    "ec2:CreateTags",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteSnapshot",
    "ec2:DeregisterImage",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress",
    "ec2:RunInstances",
    "ec2:StopInstances"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
    }
  },
  "Action" : [
    "ec2:TerminateInstances",
    "ec2:RebootInstances"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:opsworks-cm:*:*:server/*"
  ],
  "Action" : [
    "opsworks-cm:DeleteServer",

```

```
    "opsworks-cm:StartMaintenance"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/aws-opsworks-cm-*"
  ],
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:UpdateStack"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam:*:*:role/aws-opsworks-cm-*",
    "arn:aws:iam:*:*:role/service-role/aws-opsworks-cm-*"
  ],
  "Action" : [
    "iam:PassRole"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : "*",
  "Action" : [
    "acm:DeleteCertificate",
    "acm:ImportCertificate"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:UpdateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource",
```

```
    "secretsmanager:UntagResource"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ec2:DeleteTags",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:elastic-ip/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOpsWorksInstanceRegistration

AWSOpsWorksInstanceRegistration es una [política administrada por AWS](#) que: proporciona acceso a una instancia de Amazon EC2 para que se registre en una pila de OpsWorks de AWS.

Uso de la política

Puede asociar AWSOpsWorksInstanceRegistration a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de junio de 2016 a las 14:23 UTC
- Hora de edición: 3 de junio de 2016 a las 14:23 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOpsWorksRegisterCLI_EC2

AWSOpsWorksRegisterCLI_EC2 es una [política administrada por AWS](#) que: permite el registro de instancias EC2 mediante la CLI de OpsWorks

Uso de la política

Puede asociar AWSOpsWorksRegisterCLI_EC2 a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de junio de 2019 a las 15:56 UTC
- Hora de edición: 18 de junio de 2019 a las 15:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeInstances"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOpsWorksRegisterCLI_OnPremises

AWSOpsWorksRegisterCLI_OnPremises es una [política administrada por AWS](#) que: permite el registro de instancias en las instalaciones mediante la CLI de OpsWorks

Uso de la política

Puede asociar AWSOpsWorksRegisterCLI_OnPremises a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 18 de junio de 2019 a las 15:33 UTC

- Hora de edición: 18 de junio de 2019 a las 15:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  {
```

```

    "Effect" : "Allow",
    "Action" : [
      "iam:CreateGroup",
      "iam:AddUserToGroup"
    ],
    "Resource" : [
      "arn:aws:iam::*:group/AWS/OpsWorks/OpsWorks-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateUser",
      "iam:CreateAccessKey"
    ],
    "Resource" : [
      "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachUserPolicy"
    ],
    "Resource" : [
      "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
    ],
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration"
      }
    }
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOrganizationsFullAccess

AWSOrganizationsFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a AWS Organizations.

Uso de la política

Puede asociar AWSOrganizationsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de noviembre de 2018 a las 20:31 UTC
- Hora editada: 6 de febrero de 2024 a las 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource" : "*"
    },
  ],
  {
    "Sid" : "AWSOrganizationsFullAccessCreateSLR",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "organizations.amazonaws.com"
      }
    }
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSOrganizationsReadOnlyAccess

AWSOrganizationsReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a Organizations AWS .

Uso de la política

Puede asociar AWSOrganizationsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 6 de noviembre de 2018 a las 20:32 UTC
- Hora editada: 6 de febrero de 2024 a las 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
{
  "Sid" : "AWSOrganizationsReadOnlyAccount",
  "Effect" : "Allow",
  "Action" : [
    "account:GetAlternateContact",
    "account:GetContactInformation",
    "account:ListRegions"
  ],
  "Resource" : "*"
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSOrganizationsServiceTrustPolicy

AWSOrganizationsServiceTrustPolicy es una [política administrada por AWS](#) que: otorga una política que permite que AWS Organizations compartir la confianza con otros Servicios de AWS aprobados para simplificar la configuración del cliente.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de octubre de 2017 a las 23:04 UTC
- Hora de edición: 1 de noviembre de 2017 a las 06:01 UTC

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

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/organizations.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOutpostsAuthorizeServerPolicy

AWSOutpostsAuthorizeServerPolicy es una [política administrada por AWS](#) que: otorga permisos que le permiten instalar un servidor Outpost en la red en las instalaciones.

Uso de la política

Puede asociar AWSOutpostsAuthorizeServerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de enero de 2023 a las 19:23 UTC
- Hora de edición: 4 de enero de 2023 a las 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ]
    }
  ],
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSOutpostsServiceRolePolicy

AWSOutpostsServiceRolePolicy es una [política administrada por AWS](#) que: es una Política de roles vinculados al servicio para permitir el acceso a los recursos de AWS gestionados por Outposts de AWS

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de noviembre de 2020 a las 22:55 UTC
- Hora de edición: 09 de noviembre de 2020 a las 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPanoramaApplianceRolePolicy

AWSPanoramaApplianceRolePolicy es una [política administrada por AWS](#) que: permite que el software de AWS IoT de un dispositivo AWS Panorama cargue registros en Amazon CloudWatch.

Uso de la política

Puede asociar AWSPanoramaApplianceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 1 de diciembre de 2020 a las 13:13 UTC
- Hora de edición: 1 de diciembre de 2020 a las 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPanoramaApplianceServiceRolePolicy

AWSPanoramaApplianceServiceRolePolicy es una [política administrada por AWS](#) que: permite que un dispositivo AWS Panorama cargue registros en Amazon CloudWatch y obtenga objetos de los puntos de acceso de Amazon S3 creados para su uso con AWS Panorama.

Uso de la política

Puede asociar AWSPanoramaApplianceServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de octubre de 2021 a las 12:14 UTC
- Hora de edición: 17 de enero de 2023 a las 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Sid" : "PanoramaDeviceCreateLogStream",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
      "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
    ]
  },
  {
    "Sid" : "PanoramaDeviceCreateLogGroup",
    "Effect" : "Allow",
    "Action" : "logs:CreateLogGroup",
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
      "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
    ]
  },
  {
    "Sid" : "PanoramaDevicePutMetric",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "PanoramaDeviceMetrics"
      }
    }
  },
  {
    "Sid" : "PanoramaDeviceS3Access",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:GetObjectVersion"
    ],
    "Resource" : [
      "arn:aws:s3::*-nodepackage-store-*",
      "arn:aws:s3::*-application-payload-store-*",
      "arn:aws:s3:*:*:accesspoint/panorama*"
    ]
  }

```

```
    ],
    "Condition" : {
      "StringLike" : {
        "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPanoramaFullAccess

AWSPanoramaFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a Panorama de AWS

Uso de la política

Puede asociar AWSPanoramaFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2020 a las 13:12 UTC
- Hora de edición: 12 de enero de 2022 a las 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "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"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPanoramaGreengrassGroupRolePolicy

AWSPanoramaGreengrassGroupRolePolicy es una [política administrada por AWS](#) que: permite que una función de Lambda de AWS de un dispositivo AWS Panorama gestione los recursos de

Panorama, cargue registros y métricas a Amazon CloudWatch y gestione objetos en depósitos creados para su uso con Panorama.

Uso de la política

Puede asociar `AWSPanoramaGreengrassGroupRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2020 a las 13:10 UTC
- Hora de edición: 6 de enero de 2021 a las 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3::*aws-panorama*"
      ]
    }
  ]
}
```



```
    },
    {
      "Sid" : "PanoramaCloudWatchPutDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:dashboard/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "PanoramaGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPanoramaSageMakerRolePolicy

AWSPanoramaSageMakerRolePolicy es una [política administrada por AWS](#) que: permite que Amazon SageMaker gestione los objetos de los depósitos creados para su uso con Panorama de AWS.

Uso de la política

Puede asociar AWSPanoramaSageMakerRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2020 a las 13:13 UTC
- Hora de edición: 1 de diciembre de 2020 a las 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
```

```
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:GetBucket*"
    ],
    "Resource" : [
      "arn:aws:s3::*aws-panorama*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPanoramaServiceLinkedRolePolicy

AWSPanoramaServiceLinkedRolePolicy es una [política administrada por AWS](#) que: permite que AWS Panorama gestione los recursos en AWS IoT, AWS Secrets Manager y AWS Panorama.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de octubre de 2021 a las 12:12 UTC
- Hora de edición: 20 de octubre de 2021 a las 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot>DeleteThing",
        "iot>DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot>DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    }
  ]
}
```

```
]
},
{
  "Sid" : "PanoramaIoTCreateCertificateAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateKeysAndCertificate"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreatePolicy",
    "iot:CreatePolicyVersion",
    "iot:AttachPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/panorama*"
  ]
},
{
  "Sid" : "PanoramaIoTJobAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:DescribeJobExecution",
    "iot:CreateJob",
    "iot>DeleteJob"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:job/panorama*",
    "arn:aws:iot:*:*:thing/panorama*"
  ]
},
{
  "Sid" : "PanoramaIoTEndpointAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:DescribeEndpoint"
  ],
  "Resource" : [
```

```
        "*"
    ]
},
{
    "Sid" : "PanoramaReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
        "panorama:Describe*",
        "panorama:List*"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager>DeleteSecret"
    ],
    "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
    ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPanoramaServiceRolePolicy

AWSPanoramaServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Panorama gestione los recursos en Amazon S3, AWS IoT, AWS IoT GreenGrass, AWS Lambda, Amazon SageMaker y Registros de Amazon CloudWatch, y transfiera los roles de servicio a AWS IoT, AWS IoT GreenGrass y Amazon SageMaker.

Uso de la política

Puede asociar AWSPanoramaServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2020 a las 13:14 UTC
- Hora de edición: 1 de diciembre de 2020 a las 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot>DeleteThing",
        "iot>DeleteThingShadow",
        "iot:DescribeThing",
```

```

    "iot:GetThingShadow",
    "iot:UpdateThing",
    "iot:UpdateThingShadow"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/panorama*"
  ]
},
{
  "Sid" : "PanoramaIoTCertificateAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachThingPrincipal",
    "iot:DetachThingPrincipal",
    "iot:UpdateCertificate",
    "iot>DeleteCertificate",
    "iot:AttachPrincipalPolicy",
    "iot:DetachPrincipalPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/panorama*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateKeysAndCertificate",
    "iot:CreatePolicy"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreatePolicyVersion"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/panorama*"
  ]
}

```



```
},
{
  "Sid" : "PanoramaIoTJobAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:DescribeJobExecution",
    "iot:CreateJob",
    "iot>DeleteJob"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:job/panorama*",
    "arn:aws:iot:*:*:thing/panorama*"
  ]
},
{
  "Sid" : "PanoramaIoTEndpointAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:DescribeEndpoint"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaAccess",
  "Effect" : "Allow",
  "Action" : [
    "panorama:Describe*",
    "panorama>List*",
    "panorama:Get*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaS3Access",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3>DeleteObject",
    "s3>DeleteBucket",
```

```

        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
    ],
    "Resource" : [
        "arn:aws:s3::*aws-panorama*"
    ]
},
{
    "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*role/service-role/AWSPanoramaSageMakerRole"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "sagemaker.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*role/service-role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*role/service-role/AWSPanoramaGreengrassRole"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "greengrass.amazonaws.com"
            ]
        }
    }
}

```

```
    }
  },
  {
    "Sid" : "PanoramaIAMPassIoTRoleAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
      "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
    ],
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : "iot.amazonaws.com"
      }
    }
  }
},
{
  "Sid" : "PanoramaGreenGrassAccess",
  "Effect" : "Allow",
  "Action" : [
    "greengrass:AssociateRoleToGroup",
    "greengrass:AssociateServiceRoleToAccount",
    "greengrass>CreateResourceDefinition",
    "greengrass>CreateResourceDefinitionVersion",
    "greengrass>CreateCoreDefinition",
    "greengrass>CreateCoreDefinitionVersion",
    "greengrass>CreateDeployment",
    "greengrass>CreateFunctionDefinition",
    "greengrass>CreateFunctionDefinitionVersion",
    "greengrass>CreateGroup",
    "greengrass>CreateGroupCertificateAuthority",
    "greengrass>CreateGroupVersion",
    "greengrass>CreateLoggerDefinition",
    "greengrass>CreateLoggerDefinitionVersion",
    "greengrass>CreateSubscriptionDefinition",
    "greengrass>CreateSubscriptionDefinitionVersion",
    "greengrass>DeleteCoreDefinition",
    "greengrass>DeleteFunctionDefinition",
    "greengrass>DeleteResourceDefinition",
    "greengrass>DeleteGroup",
    "greengrass>DeleteLoggerDefinition",
    "greengrass>DeleteSubscriptionDefinition",
```

```
"greengrass:DisassociateRoleFromGroup",
"greengrass:DisassociateServiceRoleFromAccount",
"greengrass:GetAssociatedRole",
"greengrass:GetConnectivityInfo",
"greengrass:GetCoreDefinition",
"greengrass:GetCoreDefinitionVersion",
"greengrass:GetDeploymentStatus",
"greengrass:GetDeviceDefinition",
"greengrass:GetDeviceDefinitionVersion",
"greengrass:GetFunctionDefinition",
"greengrass:GetFunctionDefinitionVersion",
"greengrass:GetGroup",
"greengrass:GetGroupCertificateAuthority",
"greengrass:GetGroupCertificateConfiguration",
"greengrass:GetGroupVersion",
"greengrass:GetLoggerDefinition",
"greengrass:GetLoggerDefinitionVersion",
"greengrass:GetResourceDefinition",
"greengrass:GetServiceRoleForAccount",
"greengrass:GetSubscriptionDefinition",
"greengrass:GetSubscriptionDefinitionVersion",
"greengrass:ListCoreDefinitionVersions",
"greengrass:ListCoreDefinitions",
"greengrass:ListDeployments",
"greengrass:ListDeviceDefinitionVersions",
"greengrass:ListDeviceDefinitions",
"greengrass:ListFunctionDefinitionVersions",
"greengrass:ListFunctionDefinitions",
"greengrass:ListGroupCertificateAuthorities",
"greengrass:ListGroupVersions",
"greengrass:ListGroups",
"greengrass:ListLoggerDefinitionVersions",
"greengrass:ListLoggerDefinitions",
"greengrass:ListSubscriptionDefinitionVersions",
"greengrass:ListSubscriptionDefinitions",
"greengrass:ResetDeployments",
"greengrass:UpdateConnectivityInfo",
"greengrass:UpdateCoreDefinition",
"greengrass:UpdateDeviceDefinition",
"greengrass:UpdateFunctionDefinition",
"greengrass:UpdateGroup",
"greengrass:UpdateGroupCertificateConfiguration",
"greengrass:UpdateLoggerDefinition",
"greengrass:UpdateSubscriptionDefinition",
```

```
    "greengrass:UpdateResourceDefinition"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaLambdaUsersFunctionAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:*"
  ]
},
{
  "Sid" : "PanoramaSageMakerWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateTrainingJob",
    "sagemaker:StopTrainingJob",
    "sagemaker:CreateCompilationJob",
    "sagemaker:DescribeCompilationJob",
    "sagemaker:StopCompilationJob"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:training-job/panorama*",
    "arn:aws:sagemaker:*:*:compilation-job/panorama*"
  ]
},
{
  "Sid" : "PanoramaSageMakerListAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListCompilationJobs"
  ],
  "Resource" : [
    "*"
  ]
},
}
```

```
{
  "Sid" : "PanoramaSageMakerReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:DescribeTrainingJob"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:training-job/*"
  ]
},
{
  "Sid" : "PanoramaCWLogsAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachPolicy",
    "iot:CreateRoleAlias"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/panorama*",
    "arn:aws:iot:*:*:rolealias/panorama*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPriceListServiceFullAccess

`AWSPriceListServiceFullAccess` es una [política administrada por AWS](#) que: proporciona acceso total al Servicio de listas de precios de AWS.

Uso de la política

Puede asociar `AWSPriceListServiceFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de noviembre de 2017 a las 00:36 UTC
- Hora de edición: 22 de noviembre de 2017 a las 00:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPprivateCAAuditor

AWSPprivateCAAuditor es una [política administrada por AWS](#) que: proporciona al auditor acceso a una autoridad de certificación privada de AWS

Uso de la política

Puede asociar AWSPprivateCAAuditor a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de febrero de 2023 a las 18:33 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPprivateCAAuditor`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```

    "Action" : [
      "acm-pca:CreateCertificateAuthorityAuditReport",
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPRivateCAFullAccess

AWSPRivateCAFullAccess es una [política administrada por AWS](#) que: brinda acceso completo a una autoridad de certificación privada de AWS

Uso de la política

Puede asociar AWSPRivateCAFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de febrero de 2023 a las 18:20 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPrivateCAPrivilegedUser

AWSPrivateCAPrivilegedUser es una [política administrada por AWS](#) que: concede a los usuarios de certificados con privilegios acceso a una autoridad de certificación privada de AWS

Uso de la política

Puede asociar AWSPrivateCAPrivilegedUser a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de febrero de 2023 a las 18:26 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPRivateCAReADOnly

AWSPRivateCAReADOnly es una [política administrada por AWS](#) que: otorga acceso de solo lectura a una autoridad de certificación privada de AWS

Uso de la política

Puede asociar AWSPRivateCAReADOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de febrero de 2023 a las 18:30 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAReADOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
    ]
  }
}
```

```
    "acm-pca:GetCertificate",
    "acm-pca:GetPolicy",
    "acm-pca:ListPermissions",
    "acm-pca:ListTags"
  ],
  "Resource" : "*"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPriateCAUser

AWSPriateCAUser es una [política administrada por AWS](#) que: concede a los usuarios de certificados acceso a una autoridad de certificación privada de AWS

Uso de la política

Puede asociar AWSPriateCAUser a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de febrero de 2023 a las 18:16 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriateCAUser`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPrivateMarketplaceAdminFullAccess

AWSPrivateMarketplaceAdminFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a todas las acciones administrativas de un Marketplace AWS privado.

Uso de la política

Puede asociar AWSPrivateMarketplaceAdminFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2018 a las 16:32 UTC
- Hora editada: 14 de febrero de 2024 a las 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSPrivateMarketplaceRequests

AWSPrivateMarketplaceRequests es una [política administrada por AWS](#) que: brinda acceso a la creación de solicitudes en un Marketplace privado de AWS.

Uso de la política

Puede asociar `AWSPrivateMarketplaceRequests` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de octubre de 2019 a las 21:44 UTC
- Hora de edición: 28 de octubre de 2019 a las 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPrivateNetworksServiceRolePolicy

AWSPrivateNetworksServiceRolePolicy es una [política administrada por AWS](#) que: permite que Private Networks Service de AWS administre los recursos en nombre del cliente.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de diciembre de 2021 a las 23:17 UTC
- Hora de edición: 16 de diciembre de 2021 a las 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSProtonCodeBuildProvisioningBasicAccess

AWSProtonCodeBuildProvisioningBasicAccess es una [política administrada por AWS](#) que: otorga los permisos que CodeBuild necesita para ejecutar una compilación para AWS Proton CodeBuild Provisioning.

Uso de la política

Puede asociar AWSProtonCodeBuildProvisioningBasicAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 9 de noviembre de 2022 a las 21:04 UTC
- Hora de edición: 09 de noviembre de 2022 a las 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

AWSProtonCodeBuildProvisioningServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Proton administre el aprovisionamiento de recursos de Proton mediante CodeBuild y otros servicios de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de noviembre de 2022 a las 21:32 UTC
- Hora de edición: 17 de mayo de 2023 a las 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:CreateChangeSet",
    "cloudformation>DeleteChangeSet",
    "cloudformation>DeleteStack",
    "cloudformation:UpdateStack",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:ListStackResources"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "codebuild:CreateProject",
    "codebuild>DeleteProject",
    "codebuild:UpdateProject",
    "codebuild:StartBuild",
    "codebuild:StopBuild",
    "codebuild:RetryBuild",
    "codebuild:BatchGetBuilds",
    "codebuild:BatchGetProjects"
  ],
  "Resource" : "arn:aws:codebuild:*:*:project/AWSProton*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : "codebuild.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicequotas:GetServiceQuota"
  ]
}

```



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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSProtonDeveloperAccess

AWSProtonDeveloperAccess es una [política administrada por AWS](#) que: brinda acceso a las API de AWS Proton y a la consola de administración, pero no permite la administración de plantillas o entornos de Proton.

Uso de la política

Puede asociar AWSProtonDeveloperAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de febrero de 2021 a las 19:02 UTC
- Hora de edición: 18 de noviembre de 2022 a las 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSProtonFullAccess

`AWSProtonFullAccess` es una [política administrada por AWS](#) que: otorga acceso completo a las API de AWS Proton y a la Consola de administración. Además de estos permisos, también es necesario acceder a Amazon S3 para registrar las agrupaciones de plantillas de sus buckets de S3. Asimismo, se precisa acceder a Amazon IAM para crear y administrar los roles de servicio de Proton.

Uso de la política

Puede asociar `AWSProtonFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de febrero de 2021 a las 19:07 UTC
- Hora de edición: 20 de junio de 2022 a las 12:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSProtonReadOnlyAccess

AWSProtonReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a las API de AWS Proton y a la Consola de administración.

Uso de la política

Puede asociar AWSProtonReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de febrero de 2021 a las 19:09 UTC
- Hora de edición: 18 de noviembre de 2022 a las 18:28 UTC

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

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",

```

```

    "proton:ListEnvironmentAccountConnections",
    "proton:ListEnvironmentOutputs",
    "proton:ListEnvironmentProvisionedResources",
    "proton:ListEnvironments",
    "proton:ListEnvironmentTemplateMajorVersions",
    "proton:ListEnvironmentTemplateMinorVersions",
    "proton:ListEnvironmentTemplates",
    "proton:ListEnvironmentTemplateVersions",
    "proton:ListRepositories",
    "proton:ListRepositorySyncDefinitions",
    "proton:ListServiceInstanceOutputs",
    "proton:ListServiceInstanceProvisionedResources",
    "proton:ListServiceInstances",
    "proton:ListServicePipelineOutputs",
    "proton:ListServicePipelineProvisionedResources",
    "proton:ListServices",
    "proton:ListServiceTemplateMajorVersions",
    "proton:ListServiceTemplateMinorVersions",
    "proton:ListServiceTemplates",
    "proton:ListServiceTemplateVersions",
    "proton:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSProtonServiceGitSyncServiceRolePolicy

AWSProtonServiceGitSyncServiceRolePolicy es una [política administrada por AWS](#) que: permite que Proton de AWS sincronice sus definiciones de servicio, entorno y componentes desde su repositorio de git a AWS Proton.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de abril de 2023 a las 15:55 UTC
- Hora de edición: 04 de abril de 2023 a las 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
```

```
    "proton:GetServiceInstance",
    "proton:CreateServiceInstance",
    "proton:UpdateServiceInstance",
    "proton:ListServiceInstances",
    "proton:GetComponent",
    "proton:CreateComponent",
    "proton:ListComponents",
    "proton:UpdateComponent",
    "proton:GetEnvironment",
    "proton:CreateEnvironment",
    "proton:ListEnvironments",
    "proton:UpdateEnvironment"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSProtonSyncServiceRolePolicy

AWSProtonSyncServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Proton sincronice el contenido de su repositorio de git con Proton o sincronice el contenido de Proton con sus repositorios de git.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de noviembre de 2021 a las 21:14 UTC

- Hora de edición: 23 de noviembre de 2021 a las 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton>DeleteServiceTemplateVersion",
        "proton>DeleteEnvironmentTemplateVersion",
        "proton>CreateServiceTemplateVersion",
        "proton>CreateServiceTemplate",
        "proton>CreateEnvironmentTemplateVersion",
        "proton>CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton>CreateEnvironmentTemplateMajorVersion",
        "proton>CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },  
    {  
      "Sid" : "AccessGitRepos",  
      "Effect" : "Allow",  
      "Action" : [  
        "codestar-connections:UseConnection"  
      ],  
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"  
    }  
  ]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSPurchaseOrdersServiceRolePolicy

AWSPurchaseOrdersServiceRolePolicy es una [política administrada por AWS](#) que: otorga permisos para ver y modificar los pedidos de compra en la consola de facturación

Uso de la política

Puede asociar AWSPurchaseOrdersServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de mayo de 2020 a las 18:15 UTC
- Hora de edición: 17 de julio de 2023 a las 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuicksightAthenaAccess

AWSQuicksightAthenaAccess es una [política administrada por AWS](#) que: brinda acceso de Quicksight a la API de Athena y a los buckets S3 utilizados para los resultados de las consultas de Athena

Uso de la política

Puede asociar AWSQuicksightAthenaAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de diciembre de 2016 a las 02:31 UTC
- Hora de edición: 7 de julio de 2021 a las 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "athena:BatchGetQueryExecution",
    "athena:CancelQueryExecution",
    "athena:GetCatalogs",
    "athena:GetExecutionEngine",
    "athena:GetExecutionEngines",
    "athena:GetNamespace",
    "athena:GetNamespaces",
    "athena:GetQueryExecution",
    "athena:GetQueryExecutions",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetTable",
    "athena:GetTables",
    "athena:ListQueryExecutions",
    "athena:RunQuery",
    "athena:StartQueryExecution",
    "athena:StopQueryExecution",
    "athena:ListWorkGroups",
    "athena:ListEngineVersions",
    "athena:GetWorkGroup",
    "athena:GetDataCatalog",
    "athena:GetDatabase",
    "athena:GetTableMetadata",
    "athena:ListDataCatalogs",
    "athena:ListDatabases",
    "athena:ListTableMetadata"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue: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" : [
    "*"
  ]
}
]
```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuickSightDescribeRDS

AWSQuickSightDescribeRDS es una [política administrada por AWS](#) que: permite que QuickSight describa los recursos de RDS

Uso de la política

Puede asociar AWSQuickSightDescribeRDS a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de noviembre de 2015 a las 23:24 UTC
- Hora de edición: 10 de noviembre de 2015 a las 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuickSightDescribeRedshift

AWSQuickSightDescribeRedshift es una [política administrada por AWS](#) que: permite que QuickSight describa los recursos de Redshift

Uso de la política

Puede asociar AWSQuickSightDescribeRedshift a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de noviembre de 2015 a las 23:25 UTC
- Hora de edición: 10 de noviembre de 2015 a las 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuickSightElasticsearchPolicy

AWSQuickSightElasticsearchPolicy es una [política administrada por AWS](#) que: proporciona acceso a los recursos de Amazon Elasticsearch desde Amazon QuickSight

Uso de la política

Puede asociar `AWSQuickSightElasticsearchPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de septiembre de 2020 a las 17:27 UTC
- Hora de edición: 7 de septiembre de 2021 a las 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "es:DescribeElasticsearchDomain",
      "es:DescribeDomain"
    ],
    "Resource" : [
      "arn:aws:es:*:*:domain/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "es:ESHttpPost",
      "es:ESHttpGet"
    ],
    "Resource" : [
      "arn:aws:es:*:*:domain/*/_opendistro/_sql",
      "arn:aws:es:*:*:domain/*/_plugin/_sql"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuickSightIoTAnalyticsAccess

AWSQuickSightIoTAnalyticsAccess es una [política administrada por AWS](#) que: brinda a QuickSight acceso de solo lectura a los conjuntos de datos de IoT Analytics

Uso de la política

Puede asociar `AWSQuickSightIoTAnalyticsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2017 a las 17:00 UTC
- Hora de edición: 29 de noviembre de 2017 a las 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuickSightListIAM

AWSQuickSightListIAM es una [política administrada por AWS](#) que: permite que QuickSight enumere las entidades de IAM

Uso de la política

Puede asociar AWSQuickSightListIAM a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de noviembre de 2015 a las 23:25 UTC
- Hora de edición: 10 de noviembre de 2015 a las 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuicksightOpenSearchPolicy

AWSQuicksightOpenSearchPolicy es una [política administrada por AWS](#) que: proporciona acceso a los recursos de Amazon OpenSearch desde Amazon QuickSight

Uso de la política

Puede asociar AWSQuicksightOpenSearchPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de septiembre de 2021 a las 23:26 UTC
- Hora de edición: 7 de septiembre de 2021 a las 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:es:*:*:domain/*/_opendistro/_sql",
      "arn:aws:es:*:*:domain/*/_plugin/_sql"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuickSightSageMakerPolicy

AWSQuickSightSageMakerPolicy es una [política administrada por AWS](#) que: concede acceso a los recursos de Amazon SageMaker desde Amazon QuickSight

Uso de la política

Puede asociar AWSQuickSightSageMakerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de enero de 2020 a las 17:18 UTC
- Hora de edición: 30 de octubre de 2023 a las 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModels",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::quicksight-ml.*",
        "arn:aws:s3:::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::sagemaker*",
      "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  },
  {
    "Sid" : "S3BucketReadAccess",
    "Effect" : "Allow",
    "Action" : "s3:ListBucket",
    "Resource" : "arn:aws:s3:::sagemaker*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSQuickSightTimestreamPolicy

AWSQuickSightTimestreamPolicy es una [política administrada por AWS](#) que: AWS QuickSight accede a las API de AWS Timestream. Los clientes pueden asociar esta política al rol AWS QuickSight para permitir la recuperación de datos y metadatos.

Uso de la política

Puede asociar AWSQuickSightTimestreamPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 30 de septiembre de 2020 a las 21:47 UTC
- Hora de edición: 30 de septiembre de 2020 a las 21:47 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSReachabilityAnalyzerServiceRolePolicy

AWSReachabilityAnalyzerServiceRolePolicy es una [política administrada por AWS](#) que: permite a VPC Reachability Analyzer acceder a los recursos de AWS e integrarse con AWS Organizations en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de noviembre de 2022 a las 17:12 UTC
- Hora de edición: 23 de junio de 2023 a las 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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"
  ]
}
]
}

```


Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSRefactoringToolkitFullAccess

AWSRefactoringToolkitFullAccess es una [política administrada por AWS](#) que: otorga permiso para usar los servicios de AWS con la extensión de AWS Toolkit for .NET Refactoring para Microsoft Visual Studio. Está pensada para asociarse a un perfil local de AWS. La política permite cargar artefactos de aplicaciones y descargar los artefactos resultantes de Amazon S3. Permite crear aplicaciones en una imagen de contenedor utilizando, almacenar AWS CodeBuild y recuperar las imágenes de Amazon Elastic Container Registry (Amazon ECR). Además, permite implementar la aplicación en servicios de contenedores en AWS, como Amazon Elastic Container Service (Amazon ECS), permite la creación opcional de recursos de VPC, la conexión opcional a la infraestructura existente, como AWS Directory Service, y otros servicios relacionados.

Uso de la política

Puede asociar AWSRefactoringToolkitFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de octubre de 2022 a las 16:41 UTC
- Hora de edición: 18 de noviembre de 2023 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSRefactoringToolkitSidecarPolicy

AWSRefactoringToolkitSidecarPolicy es una [política administrada AWS](#) que: está destinada para que las tareas de Amazon ECS la usen. Estas tareas se crearon para probar aplicaciones en AWS con la extensión de AWS Toolkit for .NET Refactoring para Microsoft Visual Studio. La política otorga acceso para descargar artefactos de aplicaciones desde Amazon S3, comunicar el estado de la tarea mediante AWS Systems Manager y otros servicios necesarios.

Uso de la política

Puede asociar AWSRefactoringToolkitSidecarPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de octubre de 2022 a las 16:41 UTC
- Hora de edición: 29 de octubre de 2022 a las 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenControlChannel",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:CreateDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/refactoringtoolkit*"
    }
  ],
  {
```



```
    "Sid" : "S3ListBucketAccess",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket"
    ],
    "Resource" : "arn:aws:s3:::*",
    "Condition" : {
      "StringLike" : {
        "s3:prefix" : "refactoringtoolkit*"
      }
    }
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSrePostPrivateCloudWatchAccess

AWSrePostPrivateCloudWatchAccesses una [política AWS gestionada](#) que: proporciona acceso privado a Re:post para publicar datos de métricas CloudWatch

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2023 a las 16:37 UTC
- Hora de edición: 15 de noviembre de 2023 a las 16:37 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSRepostSpaceSupportOperationsPolicy

AWSRepostSpaceSupportOperationsPolicy es una [política AWS gestionada](#) que: esta política permite al servicio Re:post Space crear, gestionar y resolver los casos de Support que se crean a través de la aplicación Space.

Uso de la política

Puede asociar AWSRepostSpaceSupportOperationsPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de noviembre de 2023 a las 21:52 UTC
- Hora editada: 26 de noviembre de 2023 a las 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
```

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResilienceHubAssessmentExecutionPolicy

AWSResilienceHubAssessmentExecutionPolicy es una [política administrada por AWS](#) que: es una Política para el rol de servicio de AWS Resilience Hub que permite el acceso a otros servicios de AWS para ejecutar la evaluación.

Uso de la política

Puede asociar AWSResilienceHubAssessmentExecutionPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2023 a las 12:32 UTC
- Hora de edición: 29 de octubre de 2023 a las 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "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/*"
}
]
}
```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceAccessManagerFullAccess

AWSResourceAccessManagerFullAccess es una [política administrada por AWS](#) que: proporciona acceso completo a AWS Resource Access Manager

Uso de la política

Puede asociar AWSResourceAccessManagerFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 4 de junio de 2019 a las 17:28 UTC
- Hora de edición: 4 de junio de 2019 a las 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceAccessManagerReadOnlyAccess

AWSResourceAccessManagerReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a AWS Resource Access Manager.

Uso de la política

Puede asociar AWSResourceAccessManagerReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de diciembre de 2019 a las 20:58 UTC
- Hora de edición: 9 de diciembre de 2019 a las 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceAccessManagerResourceShareParticipantAccess

AWSResourceAccessManagerResourceShareParticipantAccess es una [política administrada por AWS](#) que: concede acceso a las API de AWS Resource Access Manager que necesita un participante en un recurso compartido.

Uso de la política

Puede asociar `AWSResourceAccessManagerResourceShareParticipantAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de diciembre de 2019 a las 20:41 UTC
- Hora de edición: 9 de diciembre de 2019 a las 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceAccessManagerServiceRolePolicy

AWSResourceAccessManagerServiceRolePolicy es una [política administrada por AWS](#) que: contiene el acceso de AWS Resource Access Manager de solo lectura a la estructura Organizations de los clientes. También, contiene permisos de IAM para eliminar el rol.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2018 a las 19:28 UTC
- Hora de edición: 14 de noviembre de 2018 a las 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceExplorerFullAccess

AWSResourceExplorerFullAccess es una [política administrada por AWS](#) que: concede permisos administrativos para acceder a los recursos de Resource Explorer, y concede permisos de solo lectura a otros servicios de AWS para brindar soporte a este acceso.

Uso de la política

Puede asociar AWSResourceExplorerFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de noviembre de 2022 a las 20:01 UTC
- Hora de edición: 14 de noviembre de 2023 a las 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
```

```
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ResourceExplorerSLRAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "resource-explorer-2.amazonaws.com"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceExplorerOrganizationsAccess

`AWSResourceExplorerOrganizationsAccess` es una [política administrada por AWS](#) que otorga permisos administrativos al Explorador de recursos, y concede permisos de solo lectura a otros servicios de AWS para brindar soporte a este acceso. El administrador de Organizations de AWS necesita estos permisos para configurar y administrar la búsqueda de varias cuentas en la consola.

Uso de la política

Puede asociar `AWSResourceExplorerOrganizationsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de noviembre de 2023 a las 17:01 UTC
- Hora de edición: 14 de noviembre de 2023 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "ResourceExplorerGetSLRAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
  },
  {
    "Sid" : "ResourceExplorerCreateSLRAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "resource-explorer-2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "OrganizationsAdministratorAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "resource-explorer-2.amazonaws.com"
        ]
      }
    }
  }
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceExplorerReadOnlyAccess

`AWSResourceExplorerReadOnlyAccess` es una [política administrada por AWS](#) que: concede permisos de solo lectura para buscar y ver los recursos de Resource Explorer, y otorga permisos de solo lectura a otros servicios AWS para brindar soporte a este acceso.

Uso de la política

Puede asociar `AWSResourceExplorerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de noviembre de 2022 a las 19:56 UTC
- Hora de edición: 14 de noviembre de 2023 a las 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceExplorerServiceRolePolicy

AWSResourceExplorerServiceRolePolicy es una [política AWS administrada](#) que: permite a Resource Explorer ver los recursos y CloudTrail eventos en su nombre para indexarlos para su búsqueda.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de octubre de 2022 a las 20:35 UTC
- Hora editada: 20 de diciembre de 2023 a las 13:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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",
"qlldb:ListJournalKinesisStreamsForLedger",
"qlldb:ListLedgers",
"rds:DescribeBlueGreenDeployments",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyEndpoints",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
```

```
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeReservedDBInstances",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeSnapshotCopyGrants",
"redshift:DescribeSnapshotSchedules",
"redshift:DescribeUsageLimits",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
"rekognition:DescribeProjects",
"resiliencehub:ListApps",
"resiliencehub:ListResiliencyPolicies",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListViews",
"resource-groups:ListGroups",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53-recovery-readiness:ListRecoveryGroups",
"route53-recovery-readiness:ListResourceSets",
"route53resolver:ListFirewallDomainLists",
"route53resolver:ListFirewallRuleGroups",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverRules",
"s3:GetBucketLocation",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListStorageLensConfigurations",
"sagemaker:ListModels",
"sagemaker:ListNotebookInstances",
"secretsmanager:ListSecrets",
"servicecatalog:ListApplications",
"servicecatalog:ListAttributeGroups",
"signer:ListSigningProfiles",
"sns:ListTopics",
"sqs:ListQueues",
```

```

    "ssm:DescribeAutomationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:DescribeMaintenanceWindows",
    "ssm:DescribeMaintenanceWindowTargets",
    "ssm:DescribeMaintenanceWindowTasks",
    "ssm:DescribeParameters",
    "ssm:DescribePatchBaselines",
    "ssm-incidents:ListResponsePlans",
    "ssm:ListAssociations",
    "ssm:ListDocuments",
    "ssm:ListInventoryEntries",
    "ssm:ListResourceDataSync",
    "states:ListActivities",
    "states:ListStateMachines",
    "timestream:ListDatabases",
    "wisdom:listAssistantAssociations",
    "wisdom:ListAssistants",
    "wisdom:listKnowledgeBases"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSResourceGroupsReadOnlyAccess

AWSResourceGroupsReadOnlyAccess es una [política administrada por AWS](#) que: es de solo lectura de Resource Groups de AWS

Uso de la política

Puede asociar AWSResourceGroupsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de marzo de 2018 a las 10:27 UTC
- Hora de edición: 5 de febrero de 2019 a las 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
```

```

    "glacier:DescribeVault",
    "glacier:ListTagsForVault",
    "kinesis:ListStreams",
    "kinesis:DescribeStream",
    "kinesis:ListTagsForStream",
    "opsworks:DescribeStacks",
    "opsworks:ListTags",
    "rds:DescribeDBInstances",
    "rds:DescribeDBSnapshots",
    "rds:ListTagsForResource",
    "redshift:DescribeClusters",
    "redshift:DescribeTags",
    "route53domains:ListDomains",
    "route53:ListHealthChecks",
    "route53:GetHealthCheck",
    "route53:ListHostedZones",
    "route53:GetHostedZone",
    "route53:ListTagsForResource",
    "storagegateway:ListGateways",
    "storagegateway:DescribeGatewayInformation",
    "storagegateway:ListTagsForResource",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTags",
    "ssm:ListDocuments"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSRoboMaker_FullAccess

`AWSRoboMaker_FullAccess` es una [política administrada por AWS](#) que: proporciona acceso total a AWS RoboMaker a través de la AWS Management Console y SDK. También, brinda acceso selecto a servicios relacionados (por ejemplo, S3 o IAM).

Uso de la política

Puede asociar `AWSRoboMaker_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de septiembre de 2020 a las 18:34 UTC
- Hora de edición: 16 de septiembre de 2021 a las 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "robomaker:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*"
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : "robomaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ecr:BatchGetImage",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : "robomaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ecr-public:DescribeImages",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : "robomaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "robomaker.amazonaws.com"
      }
    }
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSRoboMakerReadOnlyAccess

AWSRoboMakerReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AWS RoboMaker a través de la AWS Management Console y SDK

Uso de la política

Puede asociar AWSRoboMakerReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de noviembre de 2018 a las 05:30 UTC
- Hora de edición: 28 de agosto de 2020 a las 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
```

```
    "Effect" : "Allow",
    "Action" : [
      "robomaker:List*",
      "robomaker:BatchDescribe*",
      "robomaker:Describe*",
      "robomaker:Get*"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSRoboMakerServicePolicy

AWSRoboMakerServicePolicy es una [política administrada por AWS](#) que: es una política de servicio de RoboMaker

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 06:30 UTC
- Hora de edición: 11 de noviembre de 2021 a las 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
```

```
    "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
  },
  {
    "Action" : [
      "lambda:UpdateFunctionCode",
      "lambda:GetFunction",
      "lambda:UpdateFunctionConfiguration",
      "lambda>DeleteFunction",
      "lambda:ListVersionsByFunction",
      "lambda:GetAlias",
      "lambda:UpdateAlias",
      "lambda:CreateAlias",
      "lambda>DeleteAlias"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lambda.amazonaws.com",
          "robomaker.amazonaws.com"
        ]
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSRoboMakerServiceRolePolicy

AWSRoboMakerServiceRolePolicy es una [política administrada por AWS](#) que: es una política de servicio de RoboMaker

Uso de la política

Puede asociar AWSRoboMakerServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de noviembre de 2018 a las 05:33 UTC
- Hora de edición: 26 de noviembre de 2018 a las 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",

```

```

    "greengrass:CreateGroupVersion",
    "greengrass:CreateFunctionDefinition",
    "greengrass:CreateFunctionDefinitionVersion",
    "greengrass:GetDeploymentStatus",
    "greengrass:GetGroup",
    "greengrass:GetGroupVersion",
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:GetFunctionDefinitionVersion",
    "greengrass:GetAssociatedRole",
    "lambda:CreateFunction"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "lambda:UpdateFunctionCode",
    "lambda:GetFunction",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSRolesAnywhereServicePolicy

AWSRolesAnywhereServicePolicy es una [política administrada por AWS](#) que: permite que las Funciones de IAM en cualquier lugar publiquen métricas de uso y servicio en CloudWatch, y comprueben el estado de las autoridades de certificación privadas en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de julio de 2022 a las 15:26 UTC
- Hora de edición: 5 de julio de 2022 a las 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/RolesAnywhere",
          "AWS/Usage"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:DescribeCertificateAuthority"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSS3OnOutpostsServiceRolePolicy

AWSS3OnOutpostsServiceRolePolicy es una [política administrada por AWS](#) que: permite que Amazon S3 on Outposts administre los recursos de red de EC2 en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de octubre de 2023 a las 20:32 UTC
- Hora de edición: 3 de octubre de 2023 a las 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OutpostsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
      "Resource" : "*",
      "Sid" : "DescribeVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Sid" : "CreateNetworkInterface"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/CreatedBy" : "S3 On Outposts"
      }
    },
    "Sid" : "CreateTagsForCreateNetworkInterface"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AllocateAddress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:ipv4pool-ec2/*"
    ],
    "Sid" : "AllocateIpAddress"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AllocateAddress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:elastic-ip/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/CreatedBy" : "S3 On Outposts"
      }
    }
  }
}
```

```
    },
    "Sid" : "CreateTagsForAllocateIpAddress"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DisassociateAddress",
      "ec2:ReleaseAddress",
      "ec2:AssociateAddress"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
      }
    }
  },
  "Sid" : "ReleaseVpcResources"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateNetworkInterface",
        "AllocateAddress"
      ],
      "aws:RequestTag/CreatedBy" : [
        "S3 On Outposts"
      ]
    }
  },
  "Sid" : "CreateTags"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSavingsPlansFullAccess

AWSSavingsPlansFullAccess es una [política administrada por AWS](#) que: proporciona acceso total al servicio Savings Plans

Uso de la política

Puede asociar AWSSavingsPlansFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de noviembre de 2019 a las 22:45 UTC
- Hora de edición: 6 de noviembre de 2019 a las 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSavingsPlansReadOnlyAccess

AWSSavingsPlansReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio Savings Plans

Uso de la política

Puede asociar AWSSavingsPlansReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de noviembre de 2019 a las 22:45 UTC
- Hora de edición: 6 de noviembre de 2019 a las 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSecurityHubFullAccess

AWSecurityHubFullAccess es una [política administrada por AWS](#) que: proporciona acceso total para usar Security Hub de AWS.

Uso de la política

Puede asociar AWSecurityHubFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2018 a las 23:54 UTC

- Hora editada: 16 de noviembre de 2023, 21:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSecurityHubOrganizationsAccess

AWSecurityHubOrganizationsAccess es una [política administrada de AWS](#) que otorga permiso para habilitar y administrar AWS Security Hub dentro de una organización. Incluye habilitar el servicio en toda la organización y determinar una cuenta como administrador delegado para el servicio.

Uso de la política

Puede asociar AWSecurityHubOrganizationsAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de marzo de 2021 a las 20:53 UTC
- Hora editada: 16 de noviembre de 2023, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSecurityHubOrganizationsAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations: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"
  }
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSecurityHubReadOnlyAccess

AWSSecurityHubReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a los recursos AWS de Security Hub

Uso de la política

Puede asociar AWSSecurityHubReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2018 a las 01:34 UTC
- Hora editada: 22 de febrero de 2024 a las 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSecurityHubServiceRolePolicy

AWSecurityHubServiceRolePolicy es una [política administrada por AWS](#) que: es un rol vinculado a un servicio necesario para que Security Hub de AWS acceda a sus recursos.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de noviembre de 2018 a las 23:47 UTC
- Hora editada: 27 de noviembre de 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSecurityHubServiceRolePolicy`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",

```

```

    "cloudwatch:DescribeAlarmsForMetric",
    "logs:DescribeMetricFilters",
    "sns:ListSubscriptionsByTopic",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus",
    "config:DescribeConfigRules",
    "config:DescribeConfigRuleEvaluationStatus",
    "config:BatchGetResourceConfig",
    "config:SelectResourceConfig",
    "iam:GenerateCredentialReport",
    "organizations:ListAccounts",
    "config:PutEvaluations",
    "tag:GetResources",
    "iam:GetCredentialReport",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListChildren",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "securityhub:BatchDisableStandards",
    "securityhub:BatchEnableStandards",
    "securityhub:BatchUpdateStandardsControlAssociations",
    "securityhub:BatchGetSecurityControls",
    "securityhub:BatchGetStandardsControlAssociations",
    "securityhub:CreateMembers",
    "securityhub>DeleteMembers",
    "securityhub:DescribeHub",
    "securityhub:DescribeOrganizationConfiguration",
    "securityhub:DescribeStandards",
    "securityhub:DescribeStandardsControls",
    "securityhub:DisassociateFromAdministratorAccount",
    "securityhub:DisassociateMembers",
    "securityhub:DisableSecurityHub",
    "securityhub:EnableSecurityHub",
    "securityhub:GetEnabledStandards",
    "securityhub:ListStandardsControlAssociations",
    "securityhub:ListSecurityControlDefinitions",
    "securityhub:UpdateOrganizationConfiguration",
    "securityhub:UpdateSecurityControl",
    "securityhub:UpdateSecurityHubConfiguration",
    "securityhub:UpdateStandardsControl"
  ],
  "Resource" : "*"
},

```

```

{
  "Sid" : "SecurityHubServiceRoleConfigPermissions",
  "Effect" : "Allow",
  "Action" : [
    "config:PutConfigRule",
    "config>DeleteConfigRule",
    "config:GetComplianceDetailsByConfigRule"
  ],
  "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
},
{
  "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "securityhub.amazonaws.com"
      ]
    }
  }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogAdminFullAccess

AWSServiceCatalogAdminFullAccess es una [política administrada por AWS](#) que: otorga acceso completo a las capacidades de administración del catálogo de servicios

Uso de la política

Puede asociar `AWSServiceCatalogAdminFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de febrero de 2018 a las 17:19 UTC
- Hora de edición: 13 de abril de 2023 a las 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:TagResource",
```

```
    "cloudformation:CreateStackSet",
    "cloudformation:CreateStackInstances",
    "cloudformation:UpdateStackSet",
    "cloudformation:UpdateStackInstances",
    "cloudformation>DeleteStackSet",
    "cloudformation>DeleteStackInstances",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/SC-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
    "arn:aws:cloudformation:*:*:changeSet/SC-*",
    "arn:aws:cloudformation:*:*:stackset/SC-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateUploadBucket",
    "cloudformation:GetTemplateSummary",
    "cloudformation:ValidateTemplate",
    "iam:GetGroup",
    "iam:GetRole",
    "iam:GetUser",
    "iam:ListGroups",
    "iam:ListRoles",
    "iam:ListUsers",
    "servicecatalog:Get*",
    "servicecatalog:Scan*",
    "servicecatalog:Search*",
    "servicecatalog:List*",
    "servicecatalog:TagResource",
    "servicecatalog:UntagResource",
    "servicecatalog:SyncResource",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:ListDocumentVersions",
    "config:DescribeConfigurationRecorders",
```

```

    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:Accept*",
    "servicecatalog:Associate*",
    "servicecatalog:Batch*",
    "servicecatalog:Copy*",
    "servicecatalog:Create*",
    "servicecatalog>Delete*",
    "servicecatalog:Describe*",
    "servicecatalog:Disable*",
    "servicecatalog:Disassociate*",
    "servicecatalog:Enable*",
    "servicecatalog:Execute*",
    "servicecatalog:Import*",
    "servicecatalog:Provision*",
    "servicecatalog:Put*",
    "servicecatalog:Reject*",
    "servicecatalog:Terminate*",
    "servicecatalog:Update*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "servicecatalog.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
  "Condition" : {
    "StringEquals" : {

```

```
        "iam:AWSServiceName" : "orgsdatasync.servicecatalog.amazonaws.com"
    }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogAdminReadOnlyAccess

AWSServiceCatalogAdminReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a las funciones de administración de Service Catalog

Uso de la política

Puede asociar AWSServiceCatalogAdminReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de octubre de 2019 a las 18:53 UTC
- Hora de edición: 25 de octubre de 2019 a las 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:List*"
      ]
    }
  ]
}
```

```
    "servicecatalog:Describe*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:Search*",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:ListDocumentVersions",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogAppRegistryFullAccess

AWSServiceCatalogAppRegistryFullAccess es una [política administrada por AWS](#) que concede acceso total a las funciones de Service Catalog App Registry

Uso de la política

Puede asociar AWSServiceCatalogAppRegistryFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de noviembre de 2020 a las 22:25 UTC
- Hora editada: 7 de diciembre de 2023, 21:50 UTC

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

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryResourceGroupsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups>DeleteGroup",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:AssociateResource",
        "resource-groups:DisassociateResource"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AppRegistryServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/servicecatalog-appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AppRegistryOperations",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStacks",
      "servicecatalog:CreateApplication",
      "servicecatalog:GetApplication",
      "servicecatalog:UpdateApplication",
      "servicecatalog>DeleteApplication",
      "servicecatalog:ListApplications",
      "servicecatalog:AssociateResource",
      "servicecatalog:DisassociateResource",
      "servicecatalog:GetAssociatedResource",
      "servicecatalog:ListAssociatedResources",
      "servicecatalog:AssociateAttributeGroup",
      "servicecatalog:DisassociateAttributeGroup",
      "servicecatalog:ListAssociatedAttributeGroups",
      "servicecatalog:CreateAttributeGroup",
      "servicecatalog:UpdateAttributeGroup",
      "servicecatalog>DeleteAttributeGroup",
      "servicecatalog:GetAttributeGroup",
      "servicecatalog:ListAttributeGroups",
      "servicecatalog:SyncResource",
      "servicecatalog:ListAttributeGroupsForApplication",
    ]
  }
}

```



```
        "servicecatalog:GetConfiguration",
        "servicecatalog:PutConfiguration"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AppRegistryResourceTagging",
    "Effect" : "Allow",
    "Action" : [
        "servicecatalog:ListTagsForResource",
        "servicecatalog:UntagResource",
        "servicecatalog:TagResource"
    ],
    "Resource" : "arn:aws:servicecatalog:*:*:*"
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

AWSServiceCatalogAppRegistryReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a las funciones de Service Catalog App Registry

Uso de la política

Puede asociar AWSServiceCatalogAppRegistryReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 12 de noviembre de 2020 a las 22:34 UTC
- Hora de edición: 17 de noviembre de 2022 a las 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogAppRegistryServiceRolePolicy

AWSServiceCatalogAppRegistryServiceRolePolicy es una [política administrada por AWS](#) que: permite que Service Catalog AppRegistry gestione Resource Groups en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de mayo de 2021 a las 22:18 UTC
- Hora de edición: 26 de octubre de 2022 a las 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups>DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroup",
```

```
    "resource-groups:GetGroupConfiguration"
  ],
  "Resource" : [
    "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
    "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
  ]
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogEndUserFullAccess

AWSServiceCatalogEndUserFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a las capacidades del catálogo de servicios para los usuarios finales

Uso de la política

Puede asociar AWSServiceCatalogEndUserFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de febrero de 2018 a las 17:22 UTC
- Hora de edición: 10 de julio de 2019 a las 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation>DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation>DeleteStackSet",
        "cloudformation>DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
      ]
    }
  ]
}
```

```

    "arn:aws:cloudformation:*:*:stackset/SC-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:GetTemplateSummary",
    "servicecatalog:DescribeProduct",
    "servicecatalog:DescribeProductView",
    "servicecatalog:DescribeProvisioningParameters",
    "servicecatalog:ListLaunchPaths",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:SearchProducts",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog>CreateProvisionedProductPlan",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ExecuteProvisionedProductPlan",
    "servicecatalog>DeleteProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:ExecuteProvisionedProductServiceAction",
    "servicecatalog:DescribeServiceActionExecutionParameters"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "servicecatalog:userLevel" : "self"
    }
  }
}

```

```
    }  
  }  
} ]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogEndUserReadOnlyAccess

AWSServiceCatalogEndUserReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a las funciones de los usuarios finales de Service Catalog

Uso de la política

Puede asociar AWSServiceCatalogEndUserReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de octubre de 2019 a las 18:49 UTC
- Hora de edición: 25 de octubre de 2019 a las 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",

```

```
    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:DescribeServiceActionExecutionParameters"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "servicecatalog:userLevel" : "self"
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

AWSServiceCatalogOrgsDataSyncServiceRolePolicy es una [política administrada por AWS](#) que: es una Política de roles vinculados a un servicio para que AWS ServiceCatalog se sincronice con la estructura organizativa de AWS Organizations

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de abril de 2023 a las 20:48 UTC
- Hora de edición: 10 de abril de 2023 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
```

```
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceCatalogSyncServiceRolePolicy

AWSServiceCatalogSyncServiceRolePolicy es una [política administrada por AWS](#) que: concede un rol vinculado a un servicio para que AWS ServiceCatalog sincronice los artefactos de aprovisionamiento de los repositorios de origen

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2022 a las 21:20 UTC
- Hora de edición: 15 de noviembre de 2022 a las 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog>DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog>CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForAmazonEKSNodegroup

`AWSServiceRoleForAmazonEKSNodegroup` es una [política administrada por AWS](#) que requiere permisos para administrar grupos de nodos en la cuenta del cliente. Estas políticas están relacionadas con la administración de los siguientes recursos: `AutoscalingGroups`, `SecurityGroups`, `LaunchTemplates` y `InstanceProfiles`.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de noviembre de 2019 a las 01:34 UTC
- Hora editada: 4 de enero de 2024 a las 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "SharedSecurityGroupRelatedPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:DescribeInstances",
      "ec2:RevokeSecurityGroupEgress",
      "ec2>DeleteSecurityGroup"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/eks" : "*"
      }
    }
  },
  {
    "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:DescribeInstances",
      "ec2:RevokeSecurityGroupEgress",
      "ec2>DeleteSecurityGroup"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/eks:nodegroup-name" : "*"
      }
    }
  },
  {
    "Sid" : "LaunchTemplateRelatedPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteLaunchTemplate",
      "ec2>CreateLaunchTemplateVersion"
    ]
  }
]
```

```

    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/eks:nodegroup-name" : "*"
      }
    }
  },
  {
    "Sid" : "AutoscalingRelatedPermissions",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "autoscaling:CompleteLifecycleAction",
      "autoscaling:PutLifecycleHook",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:EnableMetricsCollection"
    ],
    "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/*"
      ]
    }
  }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy es una [política administrada por AWS](#) que: otorga acceso a los recursos de Systems Manager utilizados por CloudWatch Alarms

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de octubre de 2020 a las 09:49 UTC
- Hora de edición: 1 de octubre de 2020 a las 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "ssm:CreateOpsItem"
  ],
  "Resource" : "*",
  "Effect" : "Allow"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy es una [política administrada por AWS](#) que: permite que CloudWatch acceda a las métricas de RDS Performance Insights en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de septiembre de 2023 a las 09:32 UTC
- Hora de edición: 07 de septiembre de 2023 a las 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForCodeGuru-Profiler

AWSServiceRoleForCodeGuru-Profiler es una [política administrada por AWS](#) que: requiere un rol vinculado a un servicio para que el Generador de perfiles de Amazon CodeGuru envíe notificaciones en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de junio de 2020 a las 22:04 UTC
- Hora de edición: 26 de junio de 2020 a las 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuruProfiler`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForCodeWhispererPolicy

AWSServiceRoleForCodeWhispererPolicy es una [política AWS gestionada](#) que: esta función otorga permisos para acceder CodeWhisperer a los datos de tu cuenta para calcular la facturación, proporciona acceso para crear y acceder a informes de seguridad en Amazon CodeGuru y emite datos a CloudWatch.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de marzo de 2023 a las 19:39 UTC
- Hora de edición: 1 de marzo de 2024 a las 23:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ]
    }
  ],
}
```

```

    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "sid2",
    "Effect" : "Allow",
    "Action" : [
      "sso:ListProfileAssociations",
      "sso:ListProfiles",
      "sso:ListDirectoryAssociations",
      "sso:DescribeRegisteredRegions",
      "sso:GetProfile",
      "sso:GetManagedApplicationInstance",
      "sso:ListApplicationAssignments",
      "sso:DescribeInstance"
    ],
    "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"
      ]
    }
  }
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSServiceRoleForEC2ScheduledInstances

AWSServiceRoleForEC2ScheduledInstances es una [política administrada por AWS](#) que: permite que las instancias programadas de EC2 lancen y gestionen instancias puntuales.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de octubre de 2017 a las 18:31 UTC
- Hora de edición: 12 de octubre de 2017 a las 18:31 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
        }
      }
    }
  ]
}
```

```
}  
  }  
] }  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy es una [política administrada por AWS](#) por la que: GroundStation de AWS utiliza este rol vinculado a un servicio para invocar EC2 con el fin de buscar direcciones IPv4 públicas

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de diciembre de 2022 a las 23:52 UTC
- Hora de edición: 13 de diciembre de 2022 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForImageBuilder

AWSServiceRoleForImageBuilder es una [política administrada por AWS](#) que: permite que EC2ImageBuilder llame a los servicios de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2019 a las 22:02 UTC
- Hora de edición: 19 de octubre de 2023 a las 21:30 UTC

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

Versión de la política

Versión de la política: v19 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForIoTSiteWise

AWSServiceRoleForIoTSiteWise es una [política AWS gestionada](#) que: permite SiteWise al AWS IoT aprovisionar y gestionar pasarelas, así como consultar datos. La política incluye los permisos de AWS Greengrass que se necesitan para realizar implementaciones en grupos, los permisos de AWS Lambda para crear y actualizar funciones con prefijo de servicio, y los permisos de AWS IoT Analytics para consultar datos de almacenes de datos.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2018 a las 19:19 UTC
- Hora de edición: 13 de noviembre de 2023 a las 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "greengrass:GetCoreDefinition",
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:GetGroup",
    "greengrass:GetGroupVersion"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowSiteWiseAccessLogGroup",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
},
{
  "Sid" : "AllowSiteWiseAccessLog",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
},
{
  "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
  "Effect" : "Allow",
  "Action" : [
    "iottwinmaker:GetWorkspace",
    "iottwinmaker:ExecuteQuery"
  ],
  "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "iottwinmaker:linkedServices" : [
        "IOTSITewise"
      ]
    }
  }
}
]

```



```
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForLogDeliveryPolicy

AWSServiceRoleForLogDeliveryPolicy es una [política administrada por AWS](#) que: permite que el Servicio de entrega de registros los entregue llamando al destino del registro en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de octubre de 2019 a las 17:31 UTC
- Hora de edición: 15 de julio de 2021 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord",
      "firehose:PutRecordBatch",
      "firehose:ListTagsForDeliveryStream"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/LogDeliveryEnabled" : "true"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForMonitronPolicy

AWSServiceRoleForMonitronPolicy es una [política administrada por AWS](#) que: concede a Amazon Monitron permisos para gestionar los recursos de AWS, incluida la asignación de usuarios de SSO de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de diciembre de 2020 a las 19:06 UTC

- Hora de edición: 29 de septiembre de 2022 a las 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForNeptuneGraphPolicy

AWSServiceRoleForNeptuneGraphPolicy es una [política AWS gestionada](#) que: proporciona a Cloudwatch acceso para publicar registros y métricas operativas y de uso para Amazon Neptune

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2023 a las 14:03 UTC
- Hora editada: 29 de noviembre de 2023 a las 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GraphMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/Neptune",
        "AWS/Usage"
      ]
    }
  },
  {
    "Sid" : "GraphLogGroup",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/neptune/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "GraphLogEvents",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

AWSServiceRoleForPrivateMarketplaceAdminPolicy es una [política AWS gestionada](#) que: proporciona permisos para describir y actualizar los recursos de Private Marketplace y describir AWS las organizaciones

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de febrero de 2024 a las 22:28 UTC
- Hora editada: 14 de febrero de 2024 a las 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:DescribeEntity"
    ],
    "Resource" : [
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
    ]
  },
  {
    "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:DescribeChangeSet"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PrivateMarketplaceCatalogListPermissions",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:ListEntities",
      "aws-marketplace:ListChangeSets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:StartChangeSet"
    ],
    "Condition" : {
      "StringEquals" : {
        "catalog:ChangeType" : [
          "AssociateAudience",
          "DisassociateAudience"
        ]
      }
    }
  }
]
```

```
    },
    "Resource" : [
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    ]
  },
  {
    "Sid" : "PrivateMarketplaceOrganizationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganizationalUnit",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListChildren"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSServiceRoleForSMS

AWSServiceRoleForSMS es una [política administrada por AWS](#) que: proporciona acceso a los servicios y recursos de AWS necesarios para migrar las instancias de servicio a EC2, S3 y AWS Cloudformation.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de agosto de 2019 a las 18:39 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    }
  ]
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DeleteStack",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:DeleteChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStackResources",
    "cloudformation:GetTemplate"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ValidateTemplate",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::sms-app-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sms:CreateReplicationJob",
    "sms>DeleteReplicationJob",
```

```

    "sms:GetReplicationJobs",
    "sms:GetReplicationRuns",
    "sms:GetServers",
    "sms:ImportServerCatalog",
    "sms:StartOnDemandReplicationRun",
    "sms:UpdateReplicationJob"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ssm:*::document/AWS-RunRemoteScript",
    "arn:aws:s3:::sms-app-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ssm:resourceTag/UseForSMSApplicationValidation" : [
        "true"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:CancelCommand",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CopySnapshot"
    }
  }
}

```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CopySnapshot",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/SMSJobId" : [
        "sms-*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifySnapshotAttribute",
    "ec2>DeleteSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/SMSJobId" : [
        "sms-*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSnapshotAttribute",
    "ec2:DeregisterImage",
    "ec2:ImportImage",
    "ec2:DescribeImportImageTasks",
    "ec2:GetEbsEncryptionByDefault"
  ],
  "Resource" : "*"
}
```

```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        }
      },
      "StringLike" : {
        "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  ]
}

```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyInstanceAttribute",
    "ec2:StopInstances",
    "ec2:StartInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "applicationinsights:Describe*",
    "applicationinsights:List*",
    "cloudformation:ListStackResources"
  ],
  "Resource" : "*"
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
      "applicationinsights:CreateApplication",
      "applicationinsights:CreateComponent",
      "applicationinsights:UpdateApplication",
      "applicationinsights>DeleteApplication",
      "applicationinsights:UpdateComponentConfiguration",
      "applicationinsights>DeleteComponent"
    ],
    "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:CreateGroup",
      "resource-groups:GetGroup",
      "resource-groups:UpdateGroup",
      "resource-groups>DeleteGroup"
    ],
    "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "application-insights.amazonaws.com"
      }
    }
  }
]

```

```
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRolePolicyForBackupReports

AWSServiceRolePolicyForBackupReports es una [política administrada por AWS](#) que: concede permisos de Backup de AWS para crear informes de conformidad, en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de agosto de 2021 a las 21:16 UTC
- Hora de edición: 10 de marzo de 2023 a las 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "backup:DescribeFramework",
      "backup:ListBackupJobs",
      "backup:ListRestoreJobs",
      "backup:ListCopyJobs"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:DescribeConfigurationRecorders",
      "config:DescribeConfigurationRecorderStatus",
      "config:BatchGetResourceConfig",
      "config:SelectResourceConfig",
      "config:DescribeConfigurationAggregators",
      "config:SelectAggregateResourceConfig",
      "config:DescribeConfigRuleEvaluationStatus",
      "config:DescribeConfigRules",
      "s3:GetBucketLocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:GetComplianceDetailsByConfigRule",
      "config:PutConfigRule",
      "config>DeleteConfigRule"
    ],
    "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config>DeleteConfigurationAggregator",
      "config:PutConfigurationAggregator"
    ],
  },
```

```
    "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
  }
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSServiceRolePolicyForBackupRestoreTesting

AWSServiceRolePolicyForBackupRestoreTesting es una [política administrada por AWS](#) que: contiene permisos para probar las restauraciones y para limpiar los recursos creados durante las pruebas.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de noviembre de 2023 a las 23:37 UTC
- Hora editada: 14 de febrero de 2024 a las 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```

    "ec2:DescribeSnapshotTierStatus",
    "ec2:DescribeTags",
    "ec2:DescribeVolumes",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "fsx:ListTagsForResource",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeDBClusterAutomatedBackups",
    "rds:ListTagsForResource",
    "redshift:DescribeClusters"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DeleteActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteVolume",
    "ec2:TerminateInstances",
    "elasticfilesystem:DeleteFilesystem",
    "elasticfilesystem:DeleteMountTarget",
    "rds>DeleteDBCluster",
    "rds>DeleteDBInstance",
    "fsx>DeleteFileSystem",
    "fsx>DeleteVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/awsbackup-restore-test" : "false"
    }
  }
},
{
  "Sid" : "DdbDeleteActions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb>DeleteTable",
    "dynamodb>DescribeTable"
  ],

```

```

    "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "RedshiftDeleteActions",
    "Effect" : "Allow",
    "Action" : "redshift:DeleteCluster",
    "Resource" : "arn:aws:redshift:*:*:cluster/awsbackup-restore-test-*"
  },
  {
    "Sid" : "S3DeleteActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:DeleteBucket",
      "s3:GetLifecycleConfiguration",
      "s3:PutLifecycleConfiguration"
    ],
    "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "TimestreamDeleteActions",
    "Effect" : "Allow",
    "Action" : "timestream:DeleteTable",
    "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSShieldDRTAccessPolicy

AWSShieldDRTAccessPolicy es una [política administrada por AWS](#) que: otorga al equipo de respuesta de DDoS de AWS acceso limitado a su Cuenta de AWS para ayudarlo a mitigar los ataques de DDoS durante un evento de gravedad alta.

Uso de la política

Puede asociar AWSShieldDRTAccessPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2018 a las 22:29 UTC
- Hora de edición: 15 de diciembre de 2020 a las 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",

```

```

    "cloudwatch:Get*",
    "cloudwatch:List*",
    "cloudfront:GetDistribution*",
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:DescribeAccelerator",
    "ec2:DescribeRegions",
    "ec2:DescribeAddresses"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SRTManageProtections",
  "Effect" : "Allow",
  "Action" : [
    "shield:*",
    "waf:*",
    "wafv2:*",
    "waf-regional:*",
    "elasticloadbalancing:SetWebACL",
    "cloudfront:UpdateDistribution",
    "apigateway:SetWebACL"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSShieldServiceRolePolicy

AWSShieldServiceRolePolicy es una [política administrada por AWS](#) que: permite a AWS Shield acceder a los recursos de AWS en su nombre para ofrecer protección contra DDoS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2021 a las 19:17 UTC
- Hora de edición: 17 de noviembre de 2021 a las 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSSMForSAPServiceLinkedRolePolicy

AWSSSMForSAPServiceLinkedRolePolicy es una [política administrada por AWS](#) que: brinda a AWS Systems Manager para SAP los permisos necesarios para gestionar e integrar el software de SAP con AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de noviembre de 2022 a las 01:18 UTC
- Hora editada: 21 de noviembre de 2023, 03:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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_*"
    ]
  }
}

```

```
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSSMOpsInsightsServiceRolePolicy

AWSSSMOpsInsightsServiceRolePolicy es una [política administrada por AWS](#) que: es una Política de roles vinculados a un servicio AWSServiceRoleForAmazonSSM_Opsinsights

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de junio de 2021 a las 20:12 UTC
- Hora de edición: 16 de junio de 2021 a las 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSSODirectoryAdministrator

AWSSSODirectoryAdministrator es una [política administrada por AWS](#) que: concede acceso de administrador al directorio de SSO

Uso de la política

Puede asociar AWSSSODirectoryAdministrator a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 31 de octubre de 2018 a las 23:54 UTC
- Hora de edición: 20 de octubre de 2022 a las 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSSODirectoryReadOnly

AWSSSODirectoryReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura para el directorio de SSO

Uso de la política

Puede asociar AWSSSODirectoryReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 31 de octubre de 2018 a las 23:49 UTC
- Hora de edición: 16 de noviembre de 2022 a las 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSSOMasterAccountAdministrator

AWSSSOMasterAccountAdministrator es una [política administrada por AWS](#) que: proporciona acceso dentro del SSO de AWS para gestionar las cuentas de AWSOrganizations maestras y de los miembros, y la aplicación en la nube

Uso de la política

Puede asociar `AWSSSOMasterAccountAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2018 a las 20:36 UTC
- Hora de edición: 20 de octubre de 2022 a las 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSSOMemberAccountAdministrator

AWSSSOMemberAccountAdministrator es una [política administrada por AWS](#) que: brinda acceso dentro del SSO de AWS para gestionar las cuentas de AWS Organizations de los miembros y la aplicación en la nube

Uso de la política

Puede asociar AWSSSOMemberAccountAdministrator a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2018 a las 20:45 UTC
- Hora de edición: 20 de octubre de 2022 a las 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
```



```
"Effect" : "Allow",
"Action" : [
  "organizations:RegisterDelegatedAdministrator",
  "organizations:DeregisterDelegatedAdministrator"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "organizations:ServicePrincipal" : "sso.amazonaws.com"
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSSOReadOnly

AWSSSOReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a las configuraciones de SSO de AWS.

Uso de la política

Puede asociar AWSSSOReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2018 a las 20:24 UTC
- Hora de edición: 22 de agosto de 2022 a las 17:23 UTC

- ARN: `arn:aws:iam::aws:policy/AWSSS0ReadOnly`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSS0ReadOnly",
      "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" : "*"
    }
  ]
}
```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSSOServiceRolePolicy

AWSSSOServiceRolePolicy es una [política administrada por AWS](#) que: concede permisos de inicio de sesión único de AWS para gestionar los recursos de AWS, incluidas los roles de IAM, las políticas y el IdP de SAML en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de diciembre de 2017 a las 18:36 UTC
- Hora de edición: 20 de octubre de 2022 a las 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Versión de la política

Versión de la política: v17 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam>DeleteRolePermissionsBoundary"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteRole",

```

```
    "iam:DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
  ]
},
{
  "Sid" : "IAMSLRCleanupActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus",
    "iam:DeleteRole",
    "iam:GetRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
  ]
},
{
  "Sid" : "IAMSAMLProviderCreationAction",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateSAMLProvider"
  ],
  "Resource" : [
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ],
  "Condition" : {
    "StringNotEquals" : {
      "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "IAMSAMLProviderUpdateAction",
  "Effect" : "Allow",
  "Action" : [
    "iam:UpdateSAMLProvider"
  ],
  "Resource" : [
```

```

    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ]
},
{
  "Sid" : "IAMSAMLProviderCleanupActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteSAMLProvider",
    "iam:GetSAMLProvider"
  ],
  "Resource" : [
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowUnauthAppForDirectory",
  "Effect" : "Allow",
  "Action" : [
    "ds:UnauthorizeApplication"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowDescribeForDirectory",
  "Effect" : "Allow",
  "Action" : [
    "ds:DescribeDirectories",
    "ds:DescribeTrusts"
  ]
},

```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
    "Effect" : "Allow",
    "Action" : [
      "identitystore:DescribeUser",
      "identitystore:DescribeGroup",
      "identitystore:ListGroups",
      "identitystore:ListUsers"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSStepFunctionsConsoleFullAccess

AWSStepFunctionsConsoleFullAccess es una [política administrada por AWS](#) que: es una política de acceso que da acceso a la consola AWS StepFunctions a un usuario, rol, etc. Para experimentar la consola completa, además de esta política, es posible que un usuario necesite el permiso IAM:PassRole para desempeñar otros roles de IAM que pueda asumir el servicio.

Uso de la política

Puede asociar AWSStepFunctionsConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 11 de enero de 2017 a las 21:54 UTC
- Hora de edición: 12 de enero de 2017 a las 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
  ]
}
```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSStepFunctionsFullAccess

`AWSStepFunctionsFullAccess` es una [política administrada por AWS](#) que: es una política de acceso para conceder acceso a la API de AWS StepFunctions a un usuario, rol, etc. Para un obtener acceso total, además de esta política, el usuario DEBE tener el permiso `IAM:PassRole` en al menos un rol de IAM que pueda asumir el servicio.

Uso de la política

Puede asociar `AWSStepFunctionsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de enero de 2017 a las 21:51 UTC
- Hora de edición: 11 de enero de 2017 a las 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSStepFunctionsReadOnlyAccess

AWSStepFunctionsReadOnlyAccess es una [política administrada por AWS](#) que: es una política de acceso para conceder acceso de solo lectura al servicio AWS StepFunctions a un usuario, rol, etc.

Uso de la política

Puede asociar AWSStepFunctionsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de enero de 2017 a las 21:46 UTC
- Hora de edición: 10 de noviembre de 2017 a las 22:03 UTC

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

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSStorageGatewayFullAccess

AWSStorageGatewayFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Puerta de enlace del almacenamiento de AWS a través de la AWS Management Console.

Uso de la política

Puede asociar AWSStorageGatewayFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de septiembre de 2022 a las 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
```

```
    "ec2:DeleteSnapshot"
  ],
  "Resource" : "*"
},
{
  "Sid" : "fetchStorageGatewayParams",
  "Effect" : "Allow",
  "Action" : "ssm:GetParameters",
  "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSStorageGatewayReadOnlyAccess

AWSStorageGatewayReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso a la Puerta de enlace del almacenamiento de AWS a través de la AWS Management Console.

Uso de la política

Puede asociar AWSStorageGatewayReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de septiembre de 2022 a las 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSStorageGatewayServiceRolePolicy

AWSStorageGatewayServiceRolePolicy es una [política administrada por AWS](#) que: presenta un rol vinculado al servicio utilizado por la Puerta de enlace del almacenamiento de AWS para permitir la integración de otros servicios de AWS con la Puerta de enlace.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de febrero de 2021 a las 19:03 UTC
- Hora de edición: 17 de febrero de 2021 a las 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "fsx:ListTagsForResource"
    ],
    "Resource" : "arn:aws:fsx:*:*:backup/*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccesses una [política AWS gestionada](#) que: AWSSupplyChainFederationAdminAccess proporciona AWS a los usuarios federados de la cadena de AWS suministro acceso a la aplicación Cadena de suministro, incluidos los permisos necesarios para realizar acciones dentro de la aplicación Cadena AWS de suministro. La política otorga permisos administrativos a los usuarios y grupos del Centro de Identidad de IAM, y está asociada a un rol creado por AWS Supply Chain en su nombre. No debe adjuntar la AWSSupplyChainFederationAdminAccess política a ninguna otra entidad de IAM.

Uso de la política

Puede asociar AWSSupplyChainFederationAdminAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de marzo de 2023 a las 18:54 UTC
- Hora de edición: 1 de noviembre de 2023 a las 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime>DeleteChannelMembership",
        "chime>DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",

```

```
    "chime:SendChannelMessage",
    "chime:UpdateChannelReadMarker",
    "chime:UpdateAppInstanceUser"
  ],
  "Resource" : [
    "arn:aws:chime:*:*:app-instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/SCNInstanceId" : "*"
    }
  }
},
{
  "Sid" : "ChimeChannel",
  "Effect" : "Allow",
  "Action" : [
    "chime:DescribeChannel"
  ],
  "Resource" : [
    "arn:aws:chime:*:*:app-instance/*"
  ]
},
{
  "Sid" : "ChimeMessaging",
  "Effect" : "Allow",
  "Action" : [
    "chime:GetMessagingSessionEndpoint"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMIdentityCenter",
  "Effect" : "Allow",
  "Action" : [
    "sso:GetManagedApplicationInstance",
    "sso:ListDirectoryAssociations",
    "sso:AssociateProfile",
    "sso:DisassociateProfile",
    "sso:ListProfiles",
    "sso:GetProfile",
    "sso:ListProfileAssociations"
  ],
  "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"
  }
}
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSupportAccess

AWSSupportAccess es una [política administrada por AWS](#) que: permite a los usuarios acceder al Centro de AWS Support.

Uso de la política

Puede asociar AWSSupportAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSupportAppFullAccess

AWSSupportAppFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a la aplicación de AWS Support y a otros servicios necesarios, como AWS Support Service Quotas. Esta política incluye permisos para usar los servicios de soporte, de modo que el usuario pueda ponerse en contacto con AWS Support para solicitar ayuda, cambiar Service Quotas y crear los roles pertinentes vinculados al servicio.

Uso de la política

Puede asociar AWSSupportAppFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de agosto de 2022 a las 16:53 UTC
- Hora de edición: 22 de agosto de 2022 a las 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:RequestServiceQuotaIncrease",
        "support:AddAttachmentsToSet",

```



```
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:DescribeSeverityLevels",
    "support:InitiateChatForCase",
    "support:ResolveCase"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "servicequotas.amazonaws.com"
    }
  }
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSupportAppReadOnlyAccess

AWSSupportAppReadOnlyAccess es una [política administrada por AWS](#) que proporciona acceso de solo lectura a la aplicación de AWS Support.

Uso de la política

Puede asociar AWSSupportAppReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de agosto de 2022 a las 17:01 UTC
- Hora de edición: 22 de agosto de 2022 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSupportPlansFullAccess

AWSSupportPlansFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a los planes de soporte.

Uso de la política

Puede asociar AWSSupportPlansFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de septiembre de 2022 a las 18:19 UTC
- Hora de edición: 9 de mayo de 2023 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "supportplans:StartSupportPlanUpdate",
    "supportplans:CreateSupportPlanSchedule"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSupportPlansReadOnlyAccess

AWSSupportPlansReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a supportplans.

Uso de la política

Puede asociar AWSSupportPlansReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de septiembre de 2022 a las 18:08 UTC
- Hora de edición: 27 de septiembre de 2022 a las 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSupportServiceRolePolicy

AWSSupportServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Support acceda a los recursos de AWS para proporcionar servicios de facturación, administrativos y de soporte.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de abril de 2018 a las 18:04 UTC
- Hora editada: 17 de enero de 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Versión de la política

Versión de la política: v34 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
      ]
    }
  ]
}
```

```

"arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
"arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
"arn:aws:apigateway:*::/apis/*/models",
"arn:aws:apigateway:*::/apis/*/models/*",
"arn:aws:apigateway:*::/apis/*/routes",
"arn:aws:apigateway:*::/apis/*/routes/*",
"arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
"arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
"arn:aws:apigateway:*::/apis/*/stages",
"arn:aws:apigateway:*::/apis/*/stages/*",
"arn:aws:apigateway:*::/clientcertificates",
"arn:aws:apigateway:*::/clientcertificates/*",
"arn:aws:apigateway:*::/domainnames",
"arn:aws:apigateway:*::/domainnames/*",
"arn:aws:apigateway:*::/domainnames/*/apimappings",
"arn:aws:apigateway:*::/domainnames/*/apimappings/*",
"arn:aws:apigateway:*::/domainnames/*/basepathmappings",
"arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
"arn:aws:apigateway:*::/restapis",
"arn:aws:apigateway:*::/restapis/*",
"arn:aws:apigateway:*::/restapis/*/authorizers",
"arn:aws:apigateway:*::/restapis/*/authorizers/*",
"arn:aws:apigateway:*::/restapis/*/deployments",
"arn:aws:apigateway:*::/restapis/*/deployments/*",
"arn:aws:apigateway:*::/restapis/*/models",
"arn:aws:apigateway:*::/restapis/*/models/*",
"arn:aws:apigateway:*::/restapis/*/models/*/default_template",
"arn:aws:apigateway:*::/restapis/*/resources",
"arn:aws:apigateway:*::/restapis/*/resources/*",
"arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
"arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
"arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
"arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
"arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
"arn:aws:apigateway:*::/restapis/*/stages",
"arn:aws:apigateway:*::/restapis/*/stages/*",
"arn:aws:apigateway:*::/usageplans",
"arn:aws:apigateway:*::/usageplans/*",
"arn:aws:apigateway:*::/vpclinks",
"arn:aws:apigateway:*::/vpclinks/*"
]
},
{

```

```

    "Sid" : "AWSSupportDeleteRoleAccess",
    "Action" : [
      "iam:DeleteRole"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
    ]
  },
  {
    "Sid" : "AWSSupportActions",
    "Action" : [
      "access-analyzer:getAccessPreview",
      "access-analyzer:getAnalyzedResource",
      "access-analyzer:getAnalyzer",
      "access-analyzer:getArchiveRule",
      "access-analyzer:getFinding",
      "access-analyzer:getGeneratedPolicy",
      "access-analyzer:listAccessPreviewFindings",
      "access-analyzer:listAccessPreviews",
      "access-analyzer:listAnalyzedResources",
      "access-analyzer:listAnalyzers",
      "access-analyzer:listArchiveRules",
      "access-analyzer:listFindings",
      "access-analyzer:listPolicyGenerations",
      "acm-pca:describeCertificateAuthority",
      "acm-pca:describeCertificateAuthorityAuditReport",
      "acm-pca:getCertificate",
      "acm-pca:getCertificateAuthorityCertificate",
      "acm-pca:getCertificateAuthorityCsr",
      "acm-pca:listCertificateAuthorities",
      "acm-pca:listTags",
      "acm:describeCertificate",
      "acm:getAccountConfiguration",
      "acm:getCertificate",
      "acm:listCertificates",
      "acm:listTagsForCertificate",
      "airflow:getEnvironment",
      "airflow:listEnvironments",
      "airflow:listTagsForResource",
      "amplify:getApp",
      "amplify:getBackendEnvironment",
      "amplify:getBranch",

```



```
"amplify:getDomainAssociation",
"amplify:getJob",
"amplify:getWebhook",
"amplify:listApps",
"amplify:listBackendEnvironments",
"amplify:listBranches",
"amplify:listDomainAssociations",
"amplify:listWebhooks",
"amplifyuibuilder:exportComponents",
"amplifyuibuilder:exportThemes",
"appflow:describeConnectorEntity",
"appflow:describeConnectorProfiles",
"appflow:describeConnectors",
"appflow:describeFlow",
"appflow:describeFlowExecutionRecords",
"appflow:listConnectorEntities",
"appflow:listFlows",
"application-autoscaling:describeScalableTargets",
"application-autoscaling:describeScalingActivities",
"application-autoscaling:describeScalingPolicies",
"application-autoscaling:describeScheduledActions",
"applicationinsights:describeApplication",
"applicationinsights:describeComponent",
"applicationinsights:describeComponentConfiguration",
"applicationinsights:describeComponentConfigurationRecommendation",
"applicationinsights:describeLogPattern",
"applicationinsights:describeObservation",
"applicationinsights:describeProblem",
"applicationinsights:describeProblemObservations",
"applicationinsights:listApplications",
"applicationinsights:listComponents",
"applicationinsights:listConfigurationHistory",
"applicationinsights:listLogPatterns",
"applicationinsights:listLogPatternSets",
"applicationinsights:listProblems",
"appmesh:describeGatewayRoute",
"appmesh:describeMesh",
"appmesh:describeRoute",
"appmesh:describeVirtualGateway",
"appmesh:describeVirtualNode",
"appmesh:describeVirtualRouter",
"appmesh:describeVirtualService",
"appmesh:listGatewayRoutes",
"appmesh:listMeshes",
```

```
"appmesh:listRoutes",
"appmesh:listTagsForResource",
"appmesh:listVirtualGateways",
"appmesh:listVirtualNodes",
"appmesh:listVirtualRouters",
"appmesh:listVirtualServices",
"apprunner:describeAutoScalingConfiguration",
"apprunner:describeCustomDomains",
"apprunner:describeOperation",
"apprunner:describeService",
"apprunner:listAutoScalingConfigurations",
"apprunner:listConnections",
"apprunner:listOperations",
"apprunner:listServices",
"apprunner:listTagsForResource",
"appstream:describeAppBlockBuilderAppBlockAssociations",
"appstream:describeAppBlockBuilders",
"appstream:describeAppBlocks",
"appstream:describeApplicationFleetAssociations",
"appstream:describeApplications",
"appstream:describeDirectoryConfigs",
"appstream:describeEntitlements",
"appstream:describeFleets",
"appstream:describeImageBuilders",
"appstream:describeImagePermissions",
"appstream:describeImages",
"appstream:describeSessions",
"appstream:describeStacks",
"appstream:describeUsageReportSubscriptions",
"appstream:describeUsers",
"appstream:describeUserStackAssociations",
"appstream:listAssociatedFleets",
"appstream:listAssociatedStacks",
"appstream:listEntitledApplications",
"appstream:listTagsForResource",
"appsync:getApiAssociation",
"appsync:getApiCache",
"appsync:getDomainName",
"appsync:getFunction",
"appsync:getGraphQLApi",
"appsync:getIntrospectionSchema",
"appsync:getResolver",
"appsync:getSchemaCreationStatus",
"appsync:getSourceApiAssociation",
```

```
"appsync:getType",
"appsync:listDataSources",
"appsync:listDomainNames",
"appsync:listFunctions",
"appsync:listGraphQLApis",
"appsync:listResolvers",
"appsync:listResolversByFunction",
"appsync:listSourceApiAssociations",
"appsync:listTypes",
"appsync:listTypesByAssociation",
"aps:describeAlertManagerDefinition",
"aps:describeRuleGroupsNamespace",
"aps:describeWorkspace",
"aps:listRuleGroupsNamespaces",
"aps:listWorkspaces",
"athena:batchGetNamedQuery",
"athena:batchGetQueryExecution",
"athena:getCalculationExecution",
"athena:getCalculationExecutionStatus",
"athena:getDataCatalog",
"athena:getNamedQuery",
"athena:getNotebookMetadata",
"athena:getQueryExecution",
"athena:getQueryRuntimeStatistics",
"athena:getSession",
"athena:getSessionStatus",
"athena:getWorkGroup",
"athena:listApplicationDPUSizes",
"athena:listCalculationExecutions",
"athena:listDataCatalogs",
"athena:listEngineVersions",
"athena:listExecutors",
"athena:listNamedQueries",
"athena:listNotebookMetadata",
"athena:listNotebookSessions",
"athena:listQueryExecutions",
"athena:listSessions",
"athena:listTagsForResource",
"athena:listWorkGroups",
"auditmanager:getAccountStatus",
"auditmanager:getDelegations",
"auditmanager:listAssessmentFrameworks",
"auditmanager:listAssessmentReports",
"auditmanager:listAssessments",
```

```
"auditmanager:listControls",
"auditmanager:listKeywordsForDataSource",
"auditmanager:listNotifications",
"autoscaling-plans:describeScalingPlanResources",
"autoscaling-plans:describeScalingPlans",
"autoscaling-plans:getScalingPlanResourceForecastData",
"autoscaling:describeAccountLimits",
"autoscaling:describeAdjustmentTypes",
"autoscaling:describeAutoScalingGroups",
"autoscaling:describeAutoScalingInstances",
"autoscaling:describeAutoScalingNotificationTypes",
"autoscaling:describeInstanceRefreshes",
"autoscaling:describeLaunchConfigurations",
"autoscaling:describeLifecycleHooks",
"autoscaling:describeLifecycleHookTypes",
"autoscaling:describeLoadBalancers",
"autoscaling:describeLoadBalancerTargetGroups",
"autoscaling:describeMetricCollectionTypes",
"autoscaling:describeNotificationConfigurations",
"autoscaling:describePolicies",
"autoscaling:describeScalingActivities",
"autoscaling:describeScalingProcessTypes",
"autoscaling:describeScheduledActions",
"autoscaling:describeTags",
"autoscaling:describeTerminationPolicyTypes",
"autoscaling:describeWarmPool",
"backup:describeBackupJob",
"backup:describeBackupVault",
"backup:describeCopyJob",
"backup:describeFramework",
"backup:describeGlobalSettings",
"backup:describeProtectedResource",
"backup:describeRecoveryPoint",
"backup:describeRegionSettings",
"backup:describeReportJob",
"backup:describeReportPlan",
"backup:describeRestoreJob",
"backup:getBackupPlan",
"backup:getBackupPlanFromJSON",
"backup:getBackupPlanFromTemplate",
"backup:getBackupSelection",
"backup:getBackupVaultAccessPolicy",
"backup:getBackupVaultNotifications",
"backup:getLegalHold",
```

```
"backup:getRecoveryPointRestoreMetadata",
"backup:getSupportedResourceTypes",
"backup:listBackupJobs",
"backup:listBackupPlans",
"backup:listBackupPlanTemplates",
"backup:listBackupPlanVersions",
"backup:listBackupSelections",
"backup:listBackupVaults",
"backup:listCopyJobs",
"backup:listFrameworks",
"backup:listLegalHolds",
"backup:listProtectedResources",
"backup:listRecoveryPointsByBackupVault",
"backup:listRecoveryPointsByLegalHold",
"backup:listRecoveryPointsByResource",
"backup:listReportJobs",
"backup:listReportPlans",
"backup:listRestoreJobs",
"backup:listTags",
"backup-gateway:getGateway",
"backup-gateway:getHypervisor",
"backup-gateway:getHypervisorPropertyMappings",
"backup-gateway:getVirtualMachine",
"backup-gateway:listGateways",
"backup-gateway:listHypervisors",
"backup-gateway:listVirtualMachines",
"batch:describeComputeEnvironments",
"batch:describeJobDefinitions",
"batch:describeJobQueues",
"batch:describeJobs",
"batch:listJobs",
"braket:getDevice",
"braket:getQuantumTask",
"braket:searchDevices",
"braket:searchQuantumTasks",
"budgets:viewBudget",
"ce:getCostAndUsage",
"ce:getCostAndUsageWithResources",
"ce:getCostForecast",
"ce:getDimensionValues",
"ce:getReservationCoverage",
"ce:getReservationPurchaseRecommendation",
"ce:getReservationUtilization",
"ce:getRightsizingRecommendation",
```

```
"ce:getSavingsPlansCoverage",
"ce:getSavingsPlansPurchaseRecommendation",
"ce:getSavingsPlansUtilization",
"ce:getSavingsPlansUtilizationDetails",
"ce:getTags",
"chime:describeAppInstance",
"chime:getAttendee",
"chime:getGlobalSettings",
"chime:getMediaCapturePipeline",
"chime:getMediaPipeline",
"chime:getMeeting",
"chime:getProxySession",
"chime:getSipMediaApplication",
"chime:getSipRule",
"chime:getVoiceConnector",
"chime:getVoiceConnectorGroup",
"chime:getVoiceConnectorLoggingConfiguration",
"chime:listAppInstances",
"chime:listAttendees",
"chime:listChannelBans",
"chime:listChannels",
"chime:listChannelsModeratedByAppInstanceUser",
"chime:listMediaCapturePipelines",
"chime:listMediaPipelines",
"chime:listMeetings",
"chime:listSipMediaApplications",
"chime:listSipRules",
"chime:listVoiceConnectorGroups",
"chime:listVoiceConnectors",
"cleanrooms:batchGetCollaborationAnalysisTemplate",
"cleanrooms:batchGetSchema",
"cleanrooms:getAnalysisTemplate",
"cleanrooms:getCollaboration",
"cleanrooms:getCollaborationAnalysisTemplate",
"cleanrooms:getConfiguredTable",
"cleanrooms:getConfiguredTableAssociation",
"cleanrooms:getMembership",
"cleanrooms:getSchema",
"cleanrooms:listAnalysisTemplates",
"cleanrooms:listCollaborationAnalysisTemplates",
"cleanrooms:listCollaborations",
"cleanrooms:listConfiguredTableAssociations",
"cleanrooms:listConfiguredTables",
"cleanrooms:listMembers",
```

```
"cleanrooms:listMemberships",
"cleanrooms:listSchemas",
"cloud9:describeEnvironmentMemberships",
"cloud9:describeEnvironments",
"cloud9:listEnvironments",
"clouddirectory:getDirectory",
"clouddirectory:listDirectories",
"cloudformation:batchDescribeTypeConfigurations",
"cloudformation:describeAccountLimits",
"cloudformation:describeChangeSet",
"cloudformation:describeChangeSetHooks",
"cloudformation:describePublisher",
"cloudformation:describeStackEvents",
"cloudformation:describeStackInstance",
"cloudformation:describeStackResource",
"cloudformation:describeStackResources",
"cloudformation:describeStacks",
"cloudformation:describeStackSet",
"cloudformation:describeStackSetOperation",
"cloudformation:describeType",
"cloudformation:describeTypeRegistration",
"cloudformation:estimateTemplateCost",
"cloudformation:getStackPolicy",
"cloudformation:getTemplate",
"cloudformation:getTemplateSummary",
"cloudformation:listChangeSets",
"cloudformation:listExports",
"cloudformation:listImports",
"cloudformation:listStackInstances",
"cloudformation:listStackResources",
"cloudformation:listStacks",
"cloudformation:listStackSetOperationResults",
"cloudformation:listStackSetOperations",
"cloudformation:listStackSets",
"cloudformation:listTypeRegistrations",
"cloudformation:listTypes",
"cloudformation:listTypeVersions",
"cloudfront:describeFunction",
"cloudfront:getCachePolicy",
"cloudfront:getCachePolicyConfig",
"cloudfront:getCloudFrontOriginAccessIdentity",
"cloudfront:getCloudFrontOriginAccessIdentityConfig",
"cloudfront:getContinuousDeploymentPolicy",
"cloudfront:getContinuousDeploymentPolicyConfig",
```

```
"cloudfront:getDistribution",
"cloudfront:getDistributionConfig",
"cloudfront:getInvalidation",
"cloudfront:getKeyGroup",
"cloudfront:getKeyGroupConfig",
"cloudfront:getMonitoringSubscription",
"cloudfront:getOriginAccessControl",
"cloudfront:getOriginAccessControlConfig",
"cloudfront:getOriginRequestPolicy",
"cloudfront:getOriginRequestPolicyConfig",
"cloudfront:getPublicKey",
"cloudfront:getPublicKeyConfig",
"cloudfront:getRealtimeLogConfig",
"cloudfront:getStreamingDistribution",
"cloudfront:getStreamingDistributionConfig",
"cloudfront:listCachePolicies",
"cloudfront:listCloudFrontOriginAccessIdentities",
"cloudfront:listContinuousDeploymentPolicies",
"cloudfront:listDistributions",
"cloudfront:listDistributionsByCachePolicyId",
"cloudfront:listDistributionsByKeyGroup",
"cloudfront:listDistributionsByOriginRequestPolicyId",
"cloudfront:listDistributionsByRealtimeLogConfig",
"cloudfront:listDistributionsByResponseHeadersPolicyId",
"cloudfront:listDistributionsByWebACLId",
"cloudfront:listFunctions",
"cloudfront:listInvalidations",
"cloudfront:listKeyGroups",
"cloudfront:listOriginAccessControls",
"cloudfront:listOriginRequestPolicies",
"cloudfront:listPublicKeys",
"cloudfront:listRealtimeLogConfigs",
"cloudfront:listStreamingDistributions",
"cloudhsm:describeBackups",
"cloudhsm:describeClusters",
"cloudsearch:describeAnalysisSchemes",
"cloudsearch:describeAvailabilityOptions",
"cloudsearch:describeDomains",
"cloudsearch:describeExpressions",
"cloudsearch:describeIndexFields",
"cloudsearch:describeScalingParameters",
"cloudsearch:describeServiceAccessPolicies",
"cloudsearch:describeSuggesters",
"cloudsearch:listDomainNames",
```



```
"cloudtrail:describeTrails",
"cloudtrail:getEventSelectors",
"cloudtrail:getInsightSelectors",
"cloudtrail:getTrail",
"cloudtrail:getTrailStatus",
"cloudtrail:listPublicKeys",
"cloudtrail:listTags",
"cloudtrail:listTrails",
"cloudtrail:lookupEvents",
"cloudwatch:describeAlarmHistory",
"cloudwatch:describeAlarms",
"cloudwatch:describeAlarmsForMetric",
"cloudwatch:describeAnomalyDetectors",
"cloudwatch:describeInsightRules",
"cloudwatch:getDashboard",
"cloudwatch:getInsightRuleReport",
"cloudwatch:getMetricData",
"cloudwatch:getMetricStatistics",
"cloudwatch:getMetricStream",
"cloudwatch:listDashboards",
"cloudwatch:listManagedInsightRules",
"cloudwatch:listMetrics",
"cloudwatch:listMetricStreams",
"codeartifact:describeDomain",
"codeartifact:describePackageVersion",
"codeartifact:describeRepository",
"codeartifact:getDomainPermissionsPolicy",
"codeartifact:getRepositoryEndpoint",
"codeartifact:getRepositoryPermissionsPolicy",
"codeartifact:listDomains",
"codeartifact:listPackages",
"codeartifact:listPackageVersionAssets",
"codeartifact:listPackageVersions",
"codeartifact:listRepositories",
"codeartifact:listRepositoriesInDomain",
"codebuild:batchGetBuildBatches",
"codebuild:batchGetBuilds",
"codebuild:batchGetProjects",
"codebuild:listBuildBatches",
"codebuild:listBuildBatchesForProject",
"codebuild:listBuilds",
"codebuild:listBuildsForProject",
"codebuild:listCuratedEnvironmentImages",
"codebuild:listProjects",
```

```
"codebuild:listSourceCredentials",
"codecommit:batchGetRepositories",
"codecommit:getBranch",
"codecommit:getRepository",
"codecommit:getRepositoryTriggers",
"codecommit:listBranches",
"codecommit:listRepositories",
"codedeploy:batchGetApplicationRevisions",
"codedeploy:batchGetApplications",
"codedeploy:batchGetDeploymentGroups",
"codedeploy:batchGetDeploymentInstances",
"codedeploy:batchGetDeployments",
"codedeploy:batchGetDeploymentTargets",
"codedeploy:batchGetOnPremisesInstances",
"codedeploy:getApplication",
"codedeploy:getApplicationRevision",
"codedeploy:getDeployment",
"codedeploy:getDeploymentConfig",
"codedeploy:getDeploymentGroup",
"codedeploy:getDeploymentInstance",
"codedeploy:getDeploymentTarget",
"codedeploy:getOnPremisesInstance",
"codedeploy:listApplicationRevisions",
"codedeploy:listApplications",
"codedeploy:listDeploymentConfigs",
"codedeploy:listDeploymentGroups",
"codedeploy:listDeploymentInstances",
"codedeploy:listDeployments",
"codedeploy:listDeploymentTargets",
"codedeploy:listGitHubAccountTokenNames",
"codedeploy:listOnPremisesInstances",
"codepipeline:getJobDetails",
"codepipeline:getPipeline",
"codepipeline:getPipelineExecution",
"codepipeline:getPipelineState",
"codepipeline:listActionExecutions",
"codepipeline:listActionTypes",
"codepipeline:listPipelineExecutions",
"codepipeline:listPipelines",
"codepipeline:listWebhooks",
"codestar:describeProject",
"codestar:listProjects",
"codestar:listResources",
"codestar:listTeamMembers",
```

```
"codestar:listUserProfiles",
"codestar-connections:getConnection",
"codestar-connections:getHost",
"codestar-connections:listConnections",
"codestar-connections:listHosts",
"cognito-identity:describeIdentityPool",
"cognito-identity:getIdentityPoolRoles",
"cognito-identity:listIdentities",
"cognito-identity:listIdentityPools",
"cognito-idp:describeIdentityProvider",
"cognito-idp:describeResourceServer",
"cognito-idp:describeRiskConfiguration",
"cognito-idp:describeUserImportJob",
"cognito-idp:describeUserPool",
"cognito-idp:describeUserPoolClient",
"cognito-idp:describeUserPoolDomain",
"cognito-idp:getGroup",
"cognito-idp:getUICustomization",
"cognito-idp:getUserPoolMfaConfig",
"cognito-idp:listGroups",
"cognito-idp:listIdentityProviders",
"cognito-idp:listResourceServers",
"cognito-idp:listUserImportJobs",
"cognito-idp:listUserPoolClients",
"cognito-idp:listUserPools",
"cognito-sync:describeDataset",
"cognito-sync:describeIdentityPoolUsage",
"cognito-sync:describeIdentityUsage",
"cognito-sync:getCognitoEvents",
"cognito-sync:getIdentityPoolConfiguration",
"cognito-sync:listDatasets",
"cognito-sync:listIdentityPoolUsage",
"comprehend:describeDocumentClassificationJob",
"comprehend:describeDocumentClassifier",
"comprehend:describeDominantLanguageDetectionJob",
"comprehend:describeEndpoint",
"comprehend:describeEntitiesDetectionJob",
"comprehend:describeEntityRecognizer",
"comprehend:describeEventsDetectionJob",
"comprehend:describeFlywheel",
"comprehend:describeFlywheelIteration",
"comprehend:describeKeyPhrasesDetectionJob",
"comprehend:describePiiEntitiesDetectionJob",
"comprehend:describeSentimentDetectionJob",
```

```
"comprehend:describeTargetedSentimentDetectionJob",
"comprehend:describeTopicsDetectionJob",
"comprehend:listDocumentClassificationJobs",
"comprehend:listDocumentClassifiers",
"comprehend:listDominantLanguageDetectionJobs",
"comprehend:listEndpoints",
"comprehend:listEntitiesDetectionJobs",
"comprehend:listEntityRecognizers",
"comprehend:listEventsDetectionJobs",
"comprehend:listFlywheelIterationHistory",
"comprehend:listFlywheels",
"comprehend:listKeyPhrasesDetectionJobs",
"comprehend:listPiiEntitiesDetectionJobs",
"comprehend:listSentimentDetectionJobs",
"comprehend:listTargetedSentimentDetectionJobs",
"comprehend:listTopicsDetectionJobs",
"compute-optimizer:getAutoScalingGroupRecommendations",
"compute-optimizer:getEBSVolumeRecommendations",
"compute-optimizer:getEC2InstanceRecommendations",
"compute-optimizer:getEC2RecommendationProjectedMetrics",
"compute-optimizer:getECSServiceRecommendations",
"compute-optimizer:getECSServiceRecommendationProjectedMetrics",
"compute-optimizer:getEnrollmentStatus",
"compute-optimizer:getRecommendationSummaries",
"config:batchGetAggregateResourceConfig",
"config:batchGetResourceConfig",
"config:describeAggregateComplianceByConfigRules",
"config:describeAggregationAuthorizations",
"config:describeComplianceByConfigRule",
"config:describeComplianceByResource",
"config:describeConfigRuleEvaluationStatus",
"config:describeConfigRules",
"config:describeConfigurationAggregators",
"config:describeConfigurationAggregatorSourcesStatus",
"config:describeConfigurationRecorders",
"config:describeConfigurationRecorderStatus",
"config:describeConformancePackCompliance",
"config:describeConformancePacks",
"config:describeConformancePackStatus",
"config:describeDeliveryChannels",
"config:describeDeliveryChannelStatus",
"config:describeOrganizationConfigRules",
"config:describeOrganizationConfigRuleStatuses",
"config:describeOrganizationConformancePacks",
```

```
"config:describeOrganizationConformancePackStatuses",
"config:describePendingAggregationRequests",
"config:describeRemediationConfigurations",
"config:describeRemediationExceptions",
"config:describeRemediationExecutionStatus",
"config:describeRetentionConfigurations",
"config:getAggregateComplianceDetailsByConfigRule",
"config:getAggregateConfigRuleComplianceSummary",
"config:getAggregateDiscoveredResourceCounts",
"config:getAggregateResourceConfig",
"config:getComplianceDetailsByConfigRule",
"config:getComplianceDetailsByResource",
"config:getComplianceSummaryByConfigRule",
"config:getComplianceSummaryByResourceType",
"config:getConformancePackComplianceDetails",
"config:getConformancePackComplianceSummary",
"config:getDiscoveredResourceCounts",
"config:getOrganizationConfigRuleDetailedStatus",
"config:getOrganizationConformancePackDetailedStatus",
"config:getResourceConfigHistory",
"config:listAggregateDiscoveredResources",
"config:listDiscoveredResources",
"config:listTagsForResource",
"connect:describeContact",
"connect:describePhoneNumber",
"connect:describeQuickConnect",
"connect:describeUser",
"connect:getCurrentMetricData",
"connect:getMetricData",
"connect:listContactEvaluations",
"connect:listEvaluationForms",
"connect:listEvaluationFormVersions",
"connect:listPhoneNumbersV2",
"connect:listQuickConnects",
"connect:listRoutingProfiles",
"connect:listSecurityProfiles",
"connect:listUsers",
"connect:listViews",
"connect:listViewVersions",
"controltower:describeAccountFactoryConfig",
"controltower:describeCoreService",
"controltower:describeGuardrail",
"controltower:describeGuardrailForTarget",
"controltower:describeManagedAccount",
```

```
"controltower:describeSingleSignOn",
"controltower:getAvailableUpdates",
"controltower:getHomeRegion",
"controltower:getLandingZoneStatus",
"controltower:listDirectoryGroups",
"controltower:listGuardrailsForTarget",
"controltower:listGuardrailViolations",
"controltower:listManagedAccounts",
"controltower:listManagedAccountsForGuardrail",
"controltower:listManagedAccountsForParent",
"controltower:listManagedOrganizationalUnits",
"controltower:listManagedOrganizationalUnitsForGuardrail",
"databrew:describeDataset",
"databrew:describeJob",
"databrew:describeProject",
"databrew:describeRecipe",
"databrew:listDatasets",
"databrew:listJobRuns",
"databrew:listJobs",
"databrew:listProjects",
"databrew:listRecipes",
"databrew:listRecipeVersions",
"databrew:listTagsForResource",
"datapipeline:describeObjects",
"datapipeline:describePipelines",
"datapipeline:getPipelineDefinition",
"datapipeline:listPipelines",
"datapipeline:queryObjects",
"datasync:describeAgent",
"datasync:describeLocationEfs",
"datasync:describeLocationFsxLustre",
"datasync:describeLocationFsxOpenZfs",
"datasync:describeLocationFsxWindows",
"datasync:describeLocationHdfs",
"datasync:describeLocationNfs",
"datasync:describeLocationObjectStorage",
"datasync:describeLocationS3",
"datasync:describeLocationSmb",
"datasync:describeTask",
"datasync:describeTaskExecution",
"datasync:listAgents",
"datasync:listLocations",
"datasync:listTaskExecutions",
"datasync:listTasks",
```

```
"dax:describeClusters",
"dax:describeDefaultParameters",
"dax:describeEvents",
"dax:describeParameterGroups",
"dax:describeParameters",
"dax:describeSubnetGroups",
"detective:getMembers",
"detective:listGraphs",
"detective:listInvitations",
"detective:listMembers",
"devicefarm:getAccountSettings",
"devicefarm:getDevice",
"devicefarm:getDevicePool",
"devicefarm:getDevicePoolCompatibility",
"devicefarm:getJob",
"devicefarm:getProject",
"devicefarm:getRemoteAccessSession",
"devicefarm:getRun",
"devicefarm:getSuite",
"devicefarm:getTest",
"devicefarm:getTestGridProject",
"devicefarm:getTestGridSession",
"devicefarm:getUpload",
"devicefarm:listArtifacts",
"devicefarm:listDevicePools",
"devicefarm:listDevices",
"devicefarm:listJobs",
"devicefarm:listProjects",
"devicefarm:listRemoteAccessSessions",
"devicefarm:listRuns",
"devicefarm:listSamples",
"devicefarm:listSuites",
"devicefarm:listTestGridProjects",
"devicefarm:listTestGridSessionActions",
"devicefarm:listTestGridSessionArtifacts",
"devicefarm:listTestGridSessions",
"devicefarm:listTests",
"devicefarm:listUniqueProblems",
"devicefarm:listUploads",
"directconnect:describeConnectionLoa",
"directconnect:describeConnections",
"directconnect:describeConnectionsOnInterconnect",
"directconnect:describeCustomerMetadata",
"directconnect:describeDirectConnectGatewayAssociationProposals",
```

```
"directconnect:describeDirectConnectGatewayAssociations",
"directconnect:describeDirectConnectGatewayAttachments",
"directconnect:describeDirectConnectGateways",
"directconnect:describeHostedConnections",
"directconnect:describeInterconnectLoa",
"directconnect:describeInterconnects",
"directconnect:describeLags",
"directconnect:describeLoa",
"directconnect:describeLocations",
"directconnect:describeRouterConfiguration",
"directconnect:describeVirtualGateways",
"directconnect:describeVirtualInterfaces",
"dlm:getLifecyclePolicies",
"dlm:getLifecyclePolicy",
"dms:describeAccountAttributes",
"dms:describeApplicableIndividualAssessments",
"dms:describeConnections",
"dms:describeEndpoints",
"dms:describeEndpointSettings",
"dms:describeEndpointTypes",
"dms:describeEventCategories",
"dms:describeEvents",
"dms:describeEventSubscriptions",
"dms:describeFleetAdvisorCollectors",
"dms:describeFleetAdvisorDatabases",
"dms:describeFleetAdvisorLsaAnalysis",
"dms:describeFleetAdvisorSchemaObjectSummary",
"dms:describeFleetAdvisorSchemas",
"dms:describeOrderableReplicationInstances",
"dms:describePendingMaintenanceActions",
"dms:describeRefreshSchemasStatus",
"dms:describeReplicationInstances",
"dms:describeReplicationInstanceTaskLogs",
"dms:describeReplicationSubnetGroups",
"dms:describeReplicationTaskAssessmentResults",
"dms:describeReplicationTaskAssessmentRuns",
"dms:describeReplicationTaskIndividualAssessments",
"dms:describeReplicationTasks",
"dms:describeSchemas",
"dms:describeTableStatistics",
"docdb-elastic:getCluster",
"docdb-elastic:getClusterSnapshot",
"docdb-elastic:listClusters",
"docdb-elastic:listClusterSnapshots",
```



```
"drs:describeJobLogItems",
"drs:describeJobs",
"drs:describeLaunchConfigurationTemplates",
"drs:describeRecoveryInstances",
"drs:describeRecoverySnapshots",
"drs:describeReplicationConfigurationTemplates",
"drs:describeSourceNetworks",
"drs:describeSourceServers",
"drs:getLaunchConfiguration",
"drs:getReplicationConfiguration",
"drs:listExtensibleSourceServers",
"drs:listLaunchActions",
"drs:listStagingAccounts",
"ds:describeClientAuthenticationSettings",
"ds:describeConditionalForwarders",
"ds:describeDirectories",
"ds:describeDomainControllers",
"ds:describeEventTopics",
"ds:describeLDAPSSettings",
"ds:describeSharedDirectories",
"ds:describeSnapshots",
"ds:describeTrusts",
"ds:getDirectoryLimits",
"ds:getSnapshotLimits",
"ds:listIpRoutes",
"ds:listSchemaExtensions",
"ds:listTagsForResource",
"dynamodb:describeBackup",
"dynamodb:describeContinuousBackups",
"dynamodb:describeContributorInsights",
"dynamodb:describeExport",
"dynamodb:describeGlobalTable",
"dynamodb:describeImport",
"dynamodb:describeKinesisStreamingDestination",
"dynamodb:describeLimits",
"dynamodb:describeStream",
"dynamodb:describeTable",
"dynamodb:describeTimeToLive",
"dynamodb:listBackups",
"dynamodb:listContributorInsights",
"dynamodb:listExports",
"dynamodb:listGlobalTables",
"dynamodb:listImports",
"dynamodb:listStreams",
```

```
"dynamodb:listTables",
"dynamodb:listTagsOfResource",
"ec2:describeAccountAttributes",
"ec2:describeAddresses",
"ec2:describeAddressesAttribute",
"ec2:describeAddressTransfers",
"ec2:describeAggregateIdFormat",
"ec2:describeAvailabilityZones",
"ec2:describeBundleTasks",
"ec2:describeByoipCidrs",
"ec2:describeCapacityReservationFleets",
"ec2:describeCapacityReservations",
"ec2:describeCarrierGateways",
"ec2:describeClassicLinkInstances",
"ec2:describeClientVpnAuthorizationRules",
"ec2:describeClientVpnConnections",
"ec2:describeClientVpnEndpoints",
"ec2:describeClientVpnRoutes",
"ec2:describeClientVpnTargetNetworks",
"ec2:describeCoipPools",
"ec2:describeConversionTasks",
"ec2:describeCustomerGateways",
"ec2:describeDhcpOptions",
"ec2:describeEgressOnlyInternetGateways",
"ec2:describeExportImageTasks",
"ec2:describeExportTasks",
"ec2:describeFastLaunchImages",
"ec2:describeFastSnapshotRestores",
"ec2:describeFleetHistory",
"ec2:describeFleetInstances",
"ec2:describeFleets",
"ec2:describeFlowLogs",
"ec2:describeFpgaImageAttribute",
"ec2:describeFpgaImages",
"ec2:describeHostReservationOfferings",
"ec2:describeHostReservations",
"ec2:describeHosts",
"ec2:describeIamInstanceProfileAssociations",
"ec2:describeIdentityIdFormat",
"ec2:describeIdFormat",
"ec2:describeImageAttribute",
"ec2:describeImages",
"ec2:describeImportImageTasks",
"ec2:describeImportSnapshotTasks",
```

```
"ec2:describeInstanceAttribute",
"ec2:describeInstanceCreditSpecifications",
"ec2:describeInstanceEventNotificationAttributes",
"ec2:describeInstanceEventWindows",
"ec2:describeInstances",
"ec2:describeInstanceStatus",
"ec2:describeInstanceTypeOfferings",
"ec2:describeInstanceTypes",
"ec2:describeInternetGateways",
"ec2:describeIpamPools",
"ec2:describeIpams",
"ec2:describeIpamScopes",
"ec2:describeIpv6Pools",
"ec2:describeKeyPairs",
"ec2:describeLaunchTemplates",
"ec2:describeLaunchTemplateVersions",
"ec2:describeLocalGatewayRouteTables",
"ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:describeLocalGatewayRouteTableVpcAssociations",
"ec2:describeLocalGateways",
"ec2:describeLocalGatewayVirtualInterfaceGroups",
"ec2:describeLocalGatewayVirtualInterfaces",
"ec2:describeManagedPrefixLists",
"ec2:describeMovingAddresses",
"ec2:describeNatGateways",
"ec2:describeNetworkAcls",
"ec2:describeNetworkInterfaceAttribute",
"ec2:describeNetworkInterfaces",
"ec2:describePlacementGroups",
"ec2:describePrefixLists",
"ec2:describePrincipalIdFormat",
"ec2:describePublicIpv4Pools",
"ec2:describeRegions",
"ec2:describeReservedInstances",
"ec2:describeReservedInstancesListings",
"ec2:describeReservedInstancesModifications",
"ec2:describeReservedInstancesOfferings",
"ec2:describeRouteTables",
"ec2:describeScheduledInstanceAvailability",
"ec2:describeScheduledInstances",
"ec2:describeSecurityGroupReferences",
"ec2:describeSecurityGroupRules",
"ec2:describeSecurityGroups",
"ec2:describeSnapshotAttribute",
```

```
"ec2:describeSnapshots",
"ec2:describeSpotDatafeedSubscription",
"ec2:describeSpotFleetInstances",
"ec2:describeSpotFleetRequestHistory",
"ec2:describeSpotFleetRequests",
"ec2:describeSpotInstanceRequests",
"ec2:describeSpotPriceHistory",
"ec2:describeStaleSecurityGroups",
"ec2:describeStoreImageTasks",
"ec2:describeSubnets",
"ec2:describeTags",
"ec2:describeTrafficMirrorFilters",
"ec2:describeTrafficMirrorSessions",
"ec2:describeTrafficMirrorTargets",
"ec2:describeTransitGatewayAttachments",
"ec2:describeTransitGatewayConnectPeers",
"ec2:describeTransitGatewayMulticastDomains",
"ec2:describeTransitGatewayPeeringAttachments",
"ec2:describeTransitGatewayPolicyTables",
"ec2:describeTransitGatewayRouteTableAnnouncements",
"ec2:describeTransitGatewayRouteTables",
"ec2:describeTransitGateways",
"ec2:describeTransitGatewayVpcAttachments",
"ec2:describeVerifiedAccessEndpoints",
"ec2:describeVerifiedAccessGroups",
"ec2:describeVerifiedAccessInstances",
"ec2:describeVerifiedAccessTrustProviders",
"ec2:describeVolumeAttribute",
"ec2:describeVolumes",
"ec2:describeVolumesModifications",
"ec2:describeVolumeStatus",
"ec2:describeVpcAttribute",
"ec2:describeVpcClassicLink",
"ec2:describeVpcClassicLinkDnsSupport",
"ec2:describeVpcEndpointConnectionNotifications",
"ec2:describeVpcEndpointConnections",
"ec2:describeVpcEndpoints",
"ec2:describeVpcEndpointServiceConfigurations",
"ec2:describeVpcEndpointServicePermissions",
"ec2:describeVpcEndpointServices",
"ec2:describeVpcPeeringConnections",
"ec2:describeVpcs",
"ec2:describeVpnConnections",
"ec2:describeVpnGateways",
```

```
"ec2:getAssociatedIpv6PoolCidrs",
"ec2:getCapacityReservationUsage",
"ec2:getCoipPoolUsage",
"ec2:getConsoleOutput",
"ec2:getConsoleScreenshot",
"ec2:getDefaultCreditSpecification",
"ec2:getEbsDefaultKmsKeyId",
"ec2:getEbsEncryptionByDefault",
"ec2:getGroupsForCapacityReservation",
"ec2:getHostReservationPurchasePreview",
"ec2:getInstanceTypesFromInstanceRequirements",
"ec2:getIpamAddressHistory",
"ec2:getIpamPoolAllocations",
"ec2:getIpamPoolCidrs",
"ec2:getIpamResourceCidrs",
"ec2:getLaunchTemplateData",
"ec2:getManagedPrefixListAssociations",
"ec2:getManagedPrefixListEntries",
"ec2:getReservedInstancesExchangeQuote",
"ec2:getSerialConsoleAccessStatus",
"ec2:getSpotPlacementScores",
"ec2:getTransitGatewayMulticastDomainAssociations",
"ec2:getTransitGatewayPrefixListReferences",
"ec2:getVerifiedAccessEndpointPolicy",
"ec2:getVerifiedAccessGroupPolicy",
"ec2:listImagesInRecycleBin",
"ec2:listSnapshotsInRecycleBin",
"ec2:searchLocalGatewayRoutes",
"ec2:searchTransitGatewayMulticastGroups",
"ec2:searchTransitGatewayRoutes",
"ecr-public:describeImages",
"ecr-public:describeImageTags",
"ecr-public:describeRegistries",
"ecr-public:describeRepositories",
"ecr-public:getRegistryCatalogData",
"ecr-public:getRepositoryCatalogData",
"ecr-public:getRepositoryPolicy",
"ecr-public:listTagsForResource",
"ecr:batchCheckLayerAvailability",
"ecr:batchGetRepositoryScanningConfiguration",
"ecr:describeImages",
"ecr:describeImageReplicationStatus",
"ecr:describeImageScanFindings",
"ecr:describePullThroughCacheRules",
```

```
"ecr:describeRegistry",
"ecr:describeRepositories",
"ecr:getLifecyclePolicy",
"ecr:getLifecyclePolicyPreview",
"ecr:getRegistryPolicy",
"ecr:getRegistryScanningConfiguration",
"ecr:getRepositoryPolicy",
"ecr:listImages",
"ecr:listTagsForResource",
"ecs:describeCapacityProviders",
"ecs:describeClusters",
"ecs:describeContainerInstances",
"ecs:describeServices",
"ecs:describeTaskDefinition",
"ecs:describeTasks",
"ecs:describeTaskSets",
"ecs:getTaskProtection",
"ecs:listAccountSettings",
"ecs:listAttributes",
"ecs:listClusters",
"ecs:listContainerInstances",
"ecs:listServices",
"ecs:listServicesByNamespace",
"ecs:listTagsForResource",
"ecs:listTaskDefinitionFamilies",
"ecs:listTaskDefinitions",
"ecs:listTasks",
"eks:describeAccessEntry",
"eks:describeAddon",
"eks:describeAddonConfiguration",
"eks:describeAddonVersions",
"eks:describeCluster",
"eks:describeEksAnywhereSubscription",
"eks:describeFargateProfile",
"eks:describeIdentityProviderConfig",
"eks:describeNodegroup",
"eks:describeUpdate",
"eks:listAccessEntries",
"eks:listAccessPolicies",
"eks:listAddons",
"eks:listAssociatedAccessPolicies",
"eks:listClusters",
"eks:listEksAnywhereSubscriptions",
"eks:listFargateProfiles",
```

```
"eks:listIdentityProviderConfigs",
"eks:listNodegroups",
"eks:listUpdates",
"elasticache:describeCacheClusters",
"elasticache:describeCacheEngineVersions",
"elasticache:describeCacheParameterGroups",
"elasticache:describeCacheParameters",
"elasticache:describeCacheSecurityGroups",
"elasticache:describeCacheSubnetGroups",
"elasticache:describeEngineDefaultParameters",
"elasticache:describeEvents",
"elasticache:describeGlobalReplicationGroups",
"elasticache:describeReplicationGroups",
"elasticache:describeReservedCacheNodes",
"elasticache:describeReservedCacheNodesOfferings",
"elasticache:describeServerlessCaches",
"elasticache:describeServerlessCacheSnapshots",
"elasticache:describeServiceUpdates",
"elasticache:describeSnapshots",
"elasticache:describeUpdateActions",
"elasticache:describeUserGroups",
"elasticache:describeUsers",
"elasticache:listAllowedNodeTypeModifications",
"elasticache:listTagsForResource",
"elasticbeanstalk:checkDNSAvailability",
"elasticbeanstalk:describeAccountAttributes",
"elasticbeanstalk:describeApplicationVersions",
"elasticbeanstalk:describeApplications",
"elasticbeanstalk:describeConfigurationOptions",
"elasticbeanstalk:describeEnvironmentHealth",
"elasticbeanstalk:describeEnvironmentManagedActionHistory",
"elasticbeanstalk:describeEnvironmentManagedActions",
"elasticbeanstalk:describeEnvironmentResources",
"elasticbeanstalk:describeEnvironments",
"elasticbeanstalk:describeEvents",
"elasticbeanstalk:describeInstancesHealth",
"elasticbeanstalk:describePlatformVersion",
"elasticbeanstalk:listAvailableSolutionStacks",
"elasticbeanstalk:listPlatformBranches",
"elasticbeanstalk:listPlatformVersions",
"elasticbeanstalk:validateConfigurationSettings",
"elasticfilesystem:describeAccessPoints",
"elasticfilesystem:describeFileSystemPolicy",
"elasticfilesystem:describeFileSystems",
```

```
"elasticfilesystem:describeLifecycleConfiguration",
"elasticfilesystem:describeMountTargets",
"elasticfilesystem:describeMountTargetSecurityGroups",
"elasticfilesystem:describeTags",
"elasticfilesystem:listTagsForResource",
"elasticloadbalancing:describeAccountLimits",
"elasticloadbalancing:describeInstanceHealth",
"elasticloadbalancing:describeListenerCertificates",
"elasticloadbalancing:describeListeners",
"elasticloadbalancing:describeLoadBalancerAttributes",
"elasticloadbalancing:describeLoadBalancerPolicies",
"elasticloadbalancing:describeLoadBalancerPolicyTypes",
"elasticloadbalancing:describeLoadBalancers",
"elasticloadbalancing:describeRules",
"elasticloadbalancing:describeSSLPolicies",
"elasticloadbalancing:describeTags",
"elasticloadbalancing:describeTargetGroupAttributes",
"elasticloadbalancing:describeTargetGroups",
"elasticloadbalancing:describeTargetHealth",
"elasticmapreduce:describeCluster",
"elasticmapreduce:describeNotebookExecution",
"elasticmapreduce:describeReleaseLabel",
"elasticmapreduce:describeSecurityConfiguration",
"elasticmapreduce:describeStep",
"elasticmapreduce:describeStudio",
"elasticmapreduce:getAutoTerminationPolicy",
"elasticmapreduce:getBlockPublicAccessConfiguration",
"elasticmapreduce:getManagedScalingPolicy",
"elasticmapreduce:getStudioSessionMapping",
"elasticmapreduce:listBootstrapActions",
"elasticmapreduce:listClusters",
"elasticmapreduce:listInstanceFleets",
"elasticmapreduce:listInstanceGroups",
"elasticmapreduce:listInstances",
"elasticmapreduce:listNotebookExecutions",
"elasticmapreduce:listReleaseLabels",
"elasticmapreduce:listSecurityConfigurations",
"elasticmapreduce:listSteps",
"elasticmapreduce:listStudios",
"elasticmapreduce:listStudioSessionMappings",
"elastictranscoder:listJobsByPipeline",
"elastictranscoder:listJobsByStatus",
"elastictranscoder:listPipelines",
"elastictranscoder:listPresets",
```



```
"elastictranscoder:readPipeline",
"elastictranscoder:readPreset",
"emr-containers:describeJobRun",
"emr-containers:describeJobTemplate",
"emr-containers:describeManagedEndpoint",
"emr-containers:describeVirtualCluster",
"emr-containers:listJobRuns",
"emr-containers:listJobTemplates",
"emr-containers:listManagedEndpoints",
"emr-containers:listVirtualClusters",
"emr-serverless:getApplication",
"emr-serverless:getJobRun",
"emr-serverless:listApplications",
"es:describeDomain",
"es:describeDomainAutoTunes",
"es:describeDomainChangeProgress",
"es:describeDomainConfig",
"es:describeDomains",
"es:describeDryRunProgress",
"es:describeElasticsearchDomain",
"es:describeElasticsearchDomainConfig",
"es:describeElasticsearchDomains",
"es:describeInboundConnections",
"es:describeInstanceTypeLimits",
"es:describeOutboundConnections",
"es:describePackages",
"es:describeReservedInstanceOfferings",
"es:describeReservedInstances",
"es:describeVpcEndpoints",
"es:getCompatibleVersions",
"es:getPackageVersionHistory",
"es:getUpgradeHistory",
"es:getUpgradeStatus",
"es:listDomainNames",
"es:listDomainsForPackage",
"es:listInstanceTypeDetails",
"es:listPackagesForDomain",
"es:listScheduledActions",
"es:listTags",
"es:listVersions",
"es:listVpcEndpointAccess",
"es:listVpcEndpoints",
"es:listVpcEndpointsForDomain",
"evidently:getExperiment",
```

```
"evidently:getFeature",
"evidently:getLaunch",
"evidently:getProject",
"evidently:getSegment",
"evidently:listExperiments",
"evidently:listFeatures",
"evidently:listLaunches",
"evidently:listProjects",
"evidently:listSegments",
"evidently:listSegmentReferences",
"events:describeApiDestination",
"events:describeArchive",
"events:describeConnection",
"events:describeEndpoint",
"events:describeEventBus",
"events:describeEventSource",
"events:describePartnerEventSource",
"events:describeReplay",
"events:describeRule",
"events:listArchives",
"events:listApiDestinations",
"events:listConnections",
"events:listEndpoints",
"events:listEventBuses",
"events:listEventSources",
"events:listPartnerEventSourceAccounts",
"events:listPartnerEventSources",
"events:listReplays",
"events:listRuleNamesByTarget",
"events:listRules",
"events:listTargetsByRule",
"events:testEventPattern",
"firehose:describeDeliveryStream",
"firehose:listDeliveryStreams",
"fms:getAdminAccount",
"fms:getComplianceDetail",
"fms:getNotificationChannel",
"fms:getPolicy",
"fms:getProtectionStatus",
"fms:listComplianceStatus",
"fms:listMemberAccounts",
"fms:listPolicies",
"forecast:describeDataset",
"forecast:describeDatasetGroup",
```

```
"forecast:describeDatasetImportJob",
"forecast:describeForecast",
"forecast:describeForecastExportJob",
"forecast:describePredictor",
"forecast:getAccuracyMetrics",
"forecast:listDatasetGroups",
"forecast:listDatasetImportJobs",
"forecast:listDatasets",
"forecast:listForecastExportJobs",
"forecast:listForecasts",
"forecast:listPredictors",
"fsx:describeBackups",
"fsx:describeDataRepositoryAssociations",
"fsx:describeDataRepositoryTasks",
"fsx:describeFileCaches",
"fsx:describeFileSystems",
"fsx:describeSnapshots",
"fsx:describeStorageVirtualMachines",
"fsx:describeVolumes",
"fsx:listTagsForResource",
"gamelift:describeAlias",
"gamelift:describeBuild",
"gamelift:describeEC2InstanceLimits",
"gamelift:describeFleetAttributes",
"gamelift:describeFleetCapacity",
"gamelift:describeFleetEvents",
"gamelift:describeFleetLocationAttributes",
"gamelift:describeFleetLocationCapacity",
"gamelift:describeFleetLocationUtilization",
"gamelift:describeFleetPortSettings",
"gamelift:describeFleetUtilization",
"gamelift:describeGameServer",
"gamelift:describeGameServerGroup",
"gamelift:describeGameSessionDetails",
"gamelift:describeGameSessionPlacement",
"gamelift:describeGameSessionQueues",
"gamelift:describeGameSessions",
"gamelift:describeInstances",
"gamelift:describeMatchmaking",
"gamelift:describeMatchmakingConfigurations",
"gamelift:describeMatchmakingRuleSets",
"gamelift:describePlayerSessions",
"gamelift:describeRuntimeConfiguration",
"gamelift:describeScalingPolicies",
```

```
"gamelift:describeScript",
"gamelift:listAliases",
"gamelift:listBuilds",
"gamelift:listFleets",
"gamelift:listGameServerGroups",
"gamelift:listGameServers",
"gamelift:listScripts",
"gamelift:resolveAlias",
"glacier:describeJob",
"glacier:describeVault",
"glacier:getDataRetrievalPolicy",
"glacier:getVaultAccessPolicy",
"glacier:getVaultLock",
"glacier:getVaultNotifications",
"glacier:listJobs",
"glacier:listTagsForVault",
"glacier:listVaults",
"globalaccelerator:describeAccelerator",
"globalaccelerator:describeAcceleratorAttributes",
"globalaccelerator:describeEndpointGroup",
"globalaccelerator:describeListener",
"globalaccelerator:listAccelerators",
"globalaccelerator:listEndpointGroups",
"globalaccelerator:listListeners",
"glue:batchGetBlueprints",
"glue:batchGetCrawlers",
"glue:batchGetDevEndpoints",
"glue:batchGetJobs",
"glue:batchGetPartition",
"glue:batchGetTriggers",
"glue:batchGetWorkflows",
"glue:checkSchemaVersionValidity",
"glue:getBlueprint",
"glue:getBlueprintRun",
"glue:getBlueprintRuns",
"glue:getCatalogImportStatus",
"glue:getClassifier",
"glue:getClassifiers",
"glue:getColumnStatisticsForPartition",
"glue:getColumnStatisticsForTable",
"glue:getCrawler",
"glue:getCrawlerMetrics",
"glue:getCrawlers",
"glue:getCustomEntityType",
```

```
"glue:getDatabase",
"glue:getDatabases",
"glue:getDataflowGraph",
"glue:getDataQualityResult",
"glue:getDataQualityRuleRecommendationRun",
"glue:getDataQualityRuleset",
"glue:getDataQualityRulesetEvaluationRun",
"glue:getDevEndpoint",
"glue:getDevEndpoints",
"glue:getJob",
"glue:getJobRun",
"glue:getJobRuns",
"glue:getJobs",
"glue:getMapping",
"glue:getMLTaskRun",
"glue:getMLTaskRuns",
"glue:getMLTransform",
"glue:getMLTransforms",
"glue:getPartition",
"glue:getPartitionIndexes",
"glue:getPartitions",
"glue:getRegistry",
"glue:getResourcePolicies",
"glue:getResourcePolicy",
"glue:getSchema",
"glue:getSchemaByDefinition",
"glue:getSchemaVersion",
"glue:getSchemaVersionsDiff",
"glue:getSession",
"glue:getStatement",
"glue:getTable",
"glue:getTables",
"glue:getTableVersions",
"glue:getTrigger",
"glue:getTriggers",
"glue:getUserDefinedFunction",
"glue:getUserDefinedFunctions",
"glue:getWorkflow",
"glue:getWorkflowRun",
"glue:getWorkflowRuns",
"glue:listCrawlers",
"glue:listCrawls",
"glue:listDataQualityResults",
"glue:listDataQualityRuleRecommendationRuns",
```

```
"glue:listDataQualityRulesetEvaluationRuns",
"glue:listDataQualityRulesets",
"glue:listDevEndpoints",
"glue:listMLTransforms",
"glue:listRegistries",
"glue:listSchemas",
"glue:listSchemaVersions",
"glue:listSessions",
"glue:listStatements",
"glue:querySchemaVersionMetadata",
"greengrass:getConnectivityInfo",
"greengrass:getCoreDefinition",
"greengrass:getCoreDefinitionVersion",
"greengrass:getDeploymentStatus",
"greengrass:getDeviceDefinition",
"greengrass:getDeviceDefinitionVersion",
"greengrass:getFunctionDefinition",
"greengrass:getFunctionDefinitionVersion",
"greengrass:getGroup",
"greengrass:getGroupCertificateAuthority",
"greengrass:getGroupVersion",
"greengrass:getLoggerDefinition",
"greengrass:getLoggerDefinitionVersion",
"greengrass:getResourceDefinitionVersion",
"greengrass:getServiceRoleForAccount",
"greengrass:getSubscriptionDefinition",
"greengrass:getSubscriptionDefinitionVersion",
"greengrass:listCoreDefinitions",
"greengrass:listCoreDefinitionVersions",
"greengrass:listDeployments",
"greengrass:listDeviceDefinitions",
"greengrass:listDeviceDefinitionVersions",
"greengrass:listFunctionDefinitions",
"greengrass:listFunctionDefinitionVersions",
"greengrass:listGroups",
"greengrass:listGroupVersions",
"greengrass:listLoggerDefinitions",
"greengrass:listLoggerDefinitionVersions",
"greengrass:listResourceDefinitions",
"greengrass:listResourceDefinitionVersions",
"greengrass:listSubscriptionDefinitions",
"greengrass:listSubscriptionDefinitionVersions",
"guardduty:getDetector",
"guardduty:getFindings",
```

```
"guardduty:getFindingsStatistics",
"guardduty:getInvitationsCount",
"guardduty:getIPSet",
"guardduty:getMasterAccount",
"guardduty:getMembers",
"guardduty:getThreatIntelSet",
"guardduty:listDetectors",
"guardduty:listFindings",
"guardduty:listInvitations",
"guardduty:listIPSets",
"guardduty:listMembers",
"guardduty:listThreatIntelSets",
"health:describeAffectedAccountsForOrganization",
"health:describeAffectedEntities",
"health:describeAffectedEntitiesForOrganization",
"health:describeEntityAggregates",
"health:describeEntityAggregatesForOrganization",
"health:describeEventAggregates",
"health:describeEventDetails",
"health:describeEventDetailsForOrganization",
"health:describeEvents",
"health:describeEventsForOrganization",
"health:describeEventTypes",
"health:describeHealthServiceStatusForOrganization",
"iam:getAccessKeyLastUsed",
"iam:getAccountAuthorizationDetails",
"iam:getAccountPasswordPolicy",
"iam:getAccountSummary",
"iam:getContextKeysForCustomPolicy",
"iam:getContextKeysForPrincipalPolicy",
"iam:getCredentialReport",
"iam:getGroup",
"iam:getGroupPolicy",
"iam:getInstanceProfile",
"iam:getLoginProfile",
"iam:getOpenIDConnectProvider",
"iam:getPolicy",
"iam:getPolicyVersion",
"iam:getRole",
"iam:getRolePolicy",
"iam:getSAMLProvider",
"iam:getServerCertificate",
"iam:getServiceLinkedRoleDeletionStatus",
"iam:getSSHPublicKey",
```

```
"iam:getUser",
"iam:getUserPolicy",
"iam:listAccessKeys",
"iam:listAccountAliases",
"iam:listAttachedGroupPolicies",
"iam:listAttachedRolePolicies",
"iam:listAttachedUserPolicies",
"iam:listEntitiesForPolicy",
"iam:listGroupPolicies",
"iam:listGroups",
"iam:listGroupsForUser",
"iam:listInstanceProfiles",
"iam:listInstanceProfilesForRole",
"iam:listMFADevices",
"iam:listOpenIDConnectProviders",
"iam:listPolicies",
"iam:listPolicyVersions",
"iam:listRolePolicies",
"iam:listRoles",
"iam:listSAMLProviders",
"iam:listServerCertificates",
"iam:listSigningCertificates",
"iam:listSSHPublicKeys",
"iam:listUserPolicies",
"iam:listUsers",
"iam:listVirtualMFADevices",
"iam:simulateCustomPolicy",
"iam:simulatePrincipalPolicy",
"imagebuilder:getComponent",
"imagebuilder:getComponentPolicy",
"imagebuilder:getContainerRecipe",
"imagebuilder:getDistributionConfiguration",
"imagebuilder:getImage",
"imagebuilder:getImagePipeline",
"imagebuilder:getImagePolicy",
"imagebuilder:getImageRecipe",
"imagebuilder:getImageRecipePolicy",
"imagebuilder:getInfrastructureConfiguration",
"imagebuilder:getLifecycleExecution",
"imagebuilder:getLifecyclePolicy",
"imagebuilder:getWorkflowExecution",
"imagebuilder:getWorkflowStepExecution",
"imagebuilder:listComponentBuildVersions",
"imagebuilder:listComponents",
```



```
"imagebuilder:listContainerRecipes",
"imagebuilder:listDistributionConfigurations",
"imagebuilder:listImageBuildVersions",
"imagebuilder:listImagePipelineImages",
"imagebuilder:listImagePipelines",
"imagebuilder:listImageRecipes",
"imagebuilder:listImages",
"imagebuilder:listImageScanFindingAggregations",
"imagebuilder:listInfrastructureConfigurations",
"imagebuilder:listLifecycleExecutions",
"imagebuilder:listLifecycleExecutionResources",
"imagebuilder:listLifecyclePolicies",
"imagebuilder:listWorkflowExecutions",
"imagebuilder:listWorkflowStepExecutions",
"imagebuilder:listTagsForResource",
"inspector:describeAssessmentRuns",
"inspector:describeAssessmentTargets",
"inspector:describeAssessmentTemplates",
"inspector:describeCrossAccountAccessRole",
"inspector:describeResourceGroups",
"inspector:describeRulesPackages",
"inspector:getTelemetryMetadata",
"inspector:listAssessmentRunAgents",
"inspector:listAssessmentRuns",
"inspector:listAssessmentTargets",
"inspector:listAssessmentTemplates",
"inspector:listEventSubscriptions",
"inspector:listRulesPackages",
"inspector:listTagsForResource",
"inspector2:batchGetAccountStatus",
"inspector2:batchGetFreeTrialInfo",
"inspector2:describeOrganizationConfiguration",
"inspector2:getDelegatedAdminAccount",
"inspector2:getMember",
"inspector2:getSbomExport",
"inspector2:listCoverage",
"inspector2:listDelegatedAdminAccounts",
"inspector2:listFilters",
"inspector2:listFindings",
"inspector2:listMembers",
"inspector2:listUsageTotals",
"inspector-scan:scanSbom",
"internetmonitor:getMonitor",
"internetmonitor:listMonitors",
```

```
"internetmonitor:getHealthEvent",
"internetmonitor:listHealthEvents",
"iot:describeAuthorizer",
"iot:describeCACertificate",
"iot:describeCertificate",
"iot:describeDefaultAuthorizer",
"iot:describeDomainConfiguration",
"iot:describeEndpoint",
"iot:describeIndex",
"iot:describeJobExecution",
"iot:describeThing",
"iot:describeThingGroup",
"iot:describeTunnel",
"iot:getEffectivePolicies",
"iot:getIndexingConfiguration",
"iot:getLoggingOptions",
"iot:getPolicy",
"iot:getPolicyVersion",
"iot:getTopicRule",
"iot:getV2LoggingOptions",
"iot:listAttachedPolicies",
"iot:listAuthorizers",
"iot:listCACertificates",
"iot:listCertificates",
"iot:listCertificatesByCA",
"iot:listDomainConfigurations",
"iot:listJobExecutionsForJob",
"iot:listJobExecutionsForThing",
"iot:listJobs",
"iot:listNamedShadowsForThing",
"iot:listOutgoingCertificates",
"iot:listPackages",
"iot:listPackageVersions",
"iot:listPolicies",
"iot:listPolicyPrincipals",
"iot:listPolicyVersions",
"iot:listPrincipalPolicies",
"iot:listPrincipalThings",
"iot:listRoleAliases",
"iot:listTargetsForPolicy",
"iot:listThingGroups",
"iot:listThingGroupsForThing",
"iot:listThingPrincipals",
"iot:listThingRegistrationTasks",
```

```
"iot:listThings",
"iot:listThingsInThingGroup",
"iot:listThingTypes",
"iot:listTopicRules",
"iot:listTunnels",
"iot:listV2LoggingLevels",
"iotevents:describeDetector",
"iotevents:describeDetectorModel",
"iotevents:describeInput",
"iotevents:describeLoggingOptions",
"iotevents:listDetectorModels",
"iotevents:listDetectorModelVersions",
"iotevents:listDetectors",
"iotevents:listInputs",
"iotfleetwise:getCampaign",
"iotfleetwise:getDecoderManifest",
"iotfleetwise:getFleet",
"iotfleetwise:getModelManifest",
"iotfleetwise:getSignalCatalog",
"iotfleetwise:getVehicle",
"iotfleetwise:getVehicleStatus",
"iotfleetwise:listCampaigns",
"iotfleetwise:listDecoderManifests",
"iotfleetwise:listDecoderManifestNetworkInterfaces",
"iotfleetwise:listDecoderManifestSignals",
"iotfleetwise:listFleets",
"iotfleetwise:listFleetsForVehicle",
"iotfleetwise:listModelManifests",
"iotfleetwise:listModelManifestNodes",
"iotfleetwise:listSignalCatalogs",
"iotfleetwise:listSignalCatalogNodes",
"iotfleetwise:listVehicles",
"iotsitewise:describeAccessPolicy",
"iotsitewise:describeAsset",
"iotsitewise:describeAssetModel",
"iotsitewise:describeAssetProperty",
"iotsitewise:describeDashboard",
"iotsitewise:describeGateway",
"iotsitewise:describeGatewayCapabilityConfiguration",
"iotsitewise:describeLoggingOptions",
"iotsitewise:describePortal",
"iotsitewise:describeProject",
"iotsitewise:listAccessPolicies",
"iotsitewise:listAssetModels",
```

```
"iotsitewise:listAssets",
"iotsitewise:listAssociatedAssets",
"iotsitewise:listDashboards",
"iotsitewise:listGateways",
"iotsitewise:listPortals",
"iotsitewise:listProjectAssets",
"iotsitewise:listProjects",
"iottwinmaker:getComponentType",
"iottwinmaker:getEntity",
"iottwinmaker:getPricingPlan",
"iottwinmaker:getScene",
"iottwinmaker:getWorkspace",
"iottwinmaker:listComponentTypes",
"iottwinmaker:listEntities",
"iottwinmaker:listScenes",
"iottwinmaker:getSyncJob",
"iottwinmaker:listSyncJobs",
"iottwinmaker:listSyncResources",
"iottwinmaker:listWorkspaces",
"iotwireless:getDestination",
"iotwireless:getDeviceProfile",
"iotwireless:getPartnerAccount",
"iotwireless:getServiceEndpoint",
"iotwireless:getServiceProfile",
"iotwireless:getWirelessDevice",
"iotwireless:getWirelessDeviceStatistics",
"iotwireless:getWirelessGateway",
"iotwireless:getWirelessGatewayCertificate",
"iotwireless:getWirelessGatewayFirmwareInformation",
"iotwireless:getWirelessGatewayStatistics",
"iotwireless:getWirelessGatewayTask",
"iotwireless:getWirelessGatewayTaskDefinition",
"iotwireless:listDestinations",
"iotwireless:listDeviceProfiles",
"iotwireless:listPartnerAccounts",
"iotwireless:listServiceProfiles",
"iotwireless:listTagsForResource",
"iotwireless:listWirelessDevices",
"iotwireless:listWirelessGateways",
"iotwireless:listWirelessGatewayTaskDefinitions",
"ivs:getChannel",
"ivs:getRecordingConfiguration",
"ivs:getStream",
"ivs:getStreamSession",
```

```
"ivs:listChannels",
"ivs:listPlaybackKeyPairs",
"ivs:listRecordingConfigurations",
"ivs:listStreamKeys",
"ivs:listStreams",
"ivs:listStreamSessions",
"kafka:describeCluster",
"kafka:describeClusterOperation",
"kafka:describeClusterV2",
"kafka:describeConfiguration",
"kafka:describeConfigurationRevision",
"kafka:getBootstrapBrokers",
"kafka:listConfigurations",
"kafka:listConfigurationRevisions",
"kafka:listClusterOperations",
"kafka:listClusters",
"kafka:listClustersV2",
"kafka:listNodes",
"kafkaconnect:describeConnector",
"kafkaconnect:describeCustomPlugin",
"kafkaconnect:describeWorkerConfiguration",
"kafkaconnect:listConnectors",
"kafkaconnect:listCustomPlugins",
"kafkaconnect:listWorkerConfigurations",
"kendra:describeDataSource",
"kendra:describeFaq",
"kendra:describeIndex",
"kendra:listDataSources",
"kendra:listFaqs",
"kendra:listIndices",
"kinesis:describeStream",
"kinesis:describeStreamConsumer",
"kinesis:describeStreamSummary",
"kinesis:listShards",
"kinesis:listStreams",
"kinesis:listStreamConsumers",
"kinesis:listTagsForStream",
"kinesisanalytics:describeApplication",
"kinesisanalytics:describeApplicationSnapshot",
"kinesisanalytics:listApplications",
"kinesisanalytics:listApplicationSnapshots",
"kinesisvideo:describeImageGenerationConfiguration",
"kinesisvideo:describeNotificationConfiguration",
"kinesisvideo:describeSignalingChannel",
```

```
"kinesisvideo:describeStream",
"kinesisvideo:getDataEndpoint",
"kinesisvideo:getIceServerConfig",
"kinesisvideo:getSignalingChannelEndpoint",
"kinesisvideo:listSignalingChannels",
"kinesisvideo:listStreams",
"kms:describeKey",
"kms:getKeyPolicy",
"kms:getKeyRotationStatus",
"kms:listAliases",
"kms:listGrants",
"kms:listKeyPolicies",
"kms:listKeys",
"kms:listResourceTags",
"kms:listRetirableGrants",
"lambda:getAccountSettings",
"lambda:getAlias",
"lambda:getCodeSigningConfig",
"lambda:getEventSourceMapping",
"lambda:getFunction",
"lambda:getFunctionCodeSigningConfig",
"lambda:getFunctionConcurrency",
"lambda:getFunctionConfiguration",
"lambda:getFunctionEventInvokeConfig",
"lambda:getFunctionUrlConfig",
"lambda:getLayerVersion",
"lambda:getLayerVersionPolicy",
"lambda:getPolicy",
"lambda:getProvisionedConcurrencyConfig",
"lambda:getRuntimeManagementConfig",
"lambda:listAliases",
"lambda:listCodeSigningConfigs",
"lambda:listEventSourceMappings",
"lambda:listFunctionEventInvokeConfigs",
"lambda:listFunctions",
"lambda:listFunctionsByCodeSigningConfig",
"lambda:listFunctionUrlConfigs",
"lambda:listLayers",
"lambda:listLayerVersions",
"lambda:listProvisionedConcurrencyConfigs",
"lambda:listVersionsByFunction",
"launchwizard:describeProvisionedApp",
"launchwizard:describeProvisioningEvents",
"launchwizard:listProvisionedApps",
```

```
"lex:describeBot",
"lex:describeBotAlias",
"lex:describeBotLocale",
"lex:describeBotRecommendation",
"lex:describeBotVersion",
"lex:describeCustomVocabularyMetadata",
"lex:describeExport",
"lex:describeImport",
"lex:describeIntent",
"lex:describeResourcePolicy",
"lex:describeSlot",
"lex:describeSlotType",
"lex:getBot",
"lex:getBotAlias",
"lex:getBotAliases",
"lex:getBotChannelAssociation",
"lex:getBotChannelAssociations",
"lex:getBots",
"lex:getBotVersions",
"lex:getBuiltinIntent",
"lex:getBuiltinIntents",
"lex:getBuiltinSlotTypes",
"lex:getIntent",
"lex:getIntents",
"lex:getIntentVersions",
"lex:getSlotType",
"lex:getSlotTypes",
"lex:getSlotTypeVersions",
"lex:listBotAliases",
"lex:listBotLocales",
"lex:listBotRecommendations",
"lex:listBots",
"lex:listBotVersions",
"lex:listExports",
"lex:listImports",
"lex:listIntents",
"lex:listRecommendedIntents",
"lex:listSlots",
"lex:listSlotTypes",
"license-manager:getLicenseConfiguration",
"license-manager:getServiceSettings",
"license-manager:listAssociationsForLicenseConfiguration",
"license-manager:listFailuresForLicenseConfigurationOperations",
"license-manager:listLicenseConfigurations",
```

```
"license-manager:listLicenseSpecificationsForResource",
"license-manager:listResourceInventory",
"license-manager:listUsageForLicenseConfiguration",
"lightsail:getActiveNames",
"lightsail:getAlarms",
"lightsail:getAutoSnapshots",
"lightsail:getBlueprints",
"lightsail:getBucketBundles",
"lightsail:getBucketMetricData",
"lightsail:getBuckets",
"lightsail:getBundles",
"lightsail:getCertificates",
"lightsail:getContainerImages",
"lightsail:getContainerServiceDeployments",
"lightsail:getContainerServiceMetricData",
"lightsail:getContainerServicePowers",
"lightsail:getContainerServices",
"lightsail:getDisk",
"lightsail:getDisks",
"lightsail:getDiskSnapshot",
"lightsail:getDiskSnapshots",
"lightsail:getDistributionBundles",
"lightsail:getDistributionMetricData",
"lightsail:getDistributions",
"lightsail:getDomain",
"lightsail:getDomains",
"lightsail:getExportSnapshotRecords",
"lightsail:getInstance",
"lightsail:getInstanceMetricData",
"lightsail:getInstancePortStates",
"lightsail:getInstances",
"lightsail:getInstanceSnapshot",
"lightsail:getInstanceSnapshots",
"lightsail:getInstanceState",
"lightsail:getKeyPair",
"lightsail:getKeyPairs",
"lightsail:getLoadBalancer",
"lightsail:getLoadBalancerMetricData",
"lightsail:getLoadBalancers",
"lightsail:getLoadBalancerTlsCertificates",
"lightsail:getOperation",
"lightsail:getOperations",
"lightsail:getOperationsForResource",
"lightsail:getRegions",
```



```
"lightsail:getRelationalDatabase",
"lightsail:getRelationalDatabaseMetricData",
"lightsail:getRelationalDatabases",
"lightsail:getRelationalDatabaseSnapshot",
"lightsail:getRelationalDatabaseSnapshots",
"lightsail:getStaticIp",
"lightsail:getStaticIps",
"lightsail:isVpcPeered",
"logs:describeAccountPolicies",
"logs:describeDeliveries",
"logs:describeDeliveryDestinations",
"logs:describeDeliverySources",
"logs:describeDestinations",
"logs:describeExportTasks",
"logs:describeLogGroups",
"logs:describeLogStreams",
"logs:describeMetricFilters",
"logs:describeQueries",
"logs:describeQueryDefinitions",
"logs:describeResourcePolicies",
"logs:describeSubscriptionFilters",
"logs:getDataProtectionPolicy",
"logs:getDelivery",
"logs:getDeliveryDestination",
"logs:getDeliveryDestinationPolicy",
"logs:getDeliverySource",
"logs:getLogDelivery",
"logs:getLogGroupFields",
"logs:listLogDeliveries",
"logs:testMetricFilter",
"lookoutequipment:describeDataIngestionJob",
"lookoutequipment:describeDataset",
"lookoutequipment:describeInferenceScheduler",
"lookoutequipment:describeModel",
"lookoutequipment:listDataIngestionJobs",
"lookoutequipment:listDatasets",
"lookoutequipment:listInferenceExecutions",
"lookoutequipment:listInferenceSchedulers",
"lookoutequipment:listModels",
"lookoutmetrics:describeAlert",
"lookoutmetrics:describeAnomalyDetectionExecutions",
"lookoutmetrics:describeAnomalyDetector",
"lookoutmetrics:describeMetricSet",
"lookoutmetrics:getAnomalyGroup",
```

```
"lookoutmetrics:getDataQualityMetrics",
"lookoutmetrics:getFeedback",
"lookoutmetrics:getSampleData",
"lookoutmetrics:listAlerts",
"lookoutmetrics:listAnomalyDetectors",
"lookoutmetrics:listAnomalyGroupSummaries",
"lookoutmetrics:listAnomalyGroupTimeSeries",
"lookoutmetrics:listMetricSets",
"lookoutmetrics:listTagsForResource",
"machinelearning:describeBatchPredictions",
"machinelearning:describeDataSources",
"machinelearning:describeEvaluations",
"machinelearning:describeMLModels",
"machinelearning:getBatchPrediction",
"machinelearning:getDataSource",
"machinelearning:getEvaluation",
"machinelearning:getMLModel",
"macie2:getClassificationExportConfiguration",
"macie2:getCustomDataIdentifier",
"macie2:getFindings",
"macie2:getFindingStatistics",
"macie2:listClassificationJobs",
"macie2:listCustomDataIdentifiers",
"macie2:listFindings",
"managedblockchain:getMember",
"managedblockchain:getNetwork",
"managedblockchain:getNode",
"managedblockchain:listMembers",
"managedblockchain:listNetworks",
"managedblockchain:listNodes",
"mediaconnect:describeFlow",
"mediaconnect:listEntitlements",
"mediaconnect:listFlows",
"mediaconvert:describeEndpoints",
"mediaconvert:getJob",
"mediaconvert:getJobTemplate",
"mediaconvert:getPreset",
"mediaconvert:getQueue",
"mediaconvert:listJobs",
"mediaconvert:listJobTemplates",
"medialive:describeChannel",
"medialive:describeInput",
"medialive:describeInputDevice",
"medialive:describeInputSecurityGroup",
```

```
"medialive:describeMultiplex",
"medialive:describeOffering",
"medialive:describeReservation",
"medialive:describeSchedule",
"medialive:listChannels",
"medialive:listInputDevices",
"medialive:listInputs",
"medialive:listInputSecurityGroups",
"medialive:listMultiplexes",
"medialive:listOfferings",
"medialive:listReservations",
"mediapackage:describeChannel",
"mediapackage:describeOriginEndpoint",
"mediapackage:listChannels",
"mediapackage:listOriginEndpoints",
"mediastore:describeContainer",
"mediastore:getContainerPolicy",
"mediastore:getCorsPolicy",
"mediastore:listContainers",
"mediatailor:getPlaybackConfiguration",
"mediatailor:listPlaybackConfigurations",
"medical-imaging:getDatastore",
"medical-imaging:listDatastores",
"mgn:describeJobLogItems",
"mgn:describeJobs",
"mgn:describeLaunchConfigurationTemplates",
"mgn:describeReplicationConfigurationTemplates",
"mgn:describeSourceServers",
"mgn:describeVcenterClients",
"mgn:getLaunchConfiguration",
"mgn:getReplicationConfiguration",
"mgn:listApplications",
"mgn:listSourceServerActions",
"mgn:listTemplateActions",
"mgn:listWaves",
"mobiletargeting:getAdmChannel",
"mobiletargeting:getApnsChannel",
"mobiletargeting:getApnsSandboxChannel",
"mobiletargeting:getApnsVoipChannel",
"mobiletargeting:getApnsVoipSandboxChannel",
"mobiletargeting:getApp",
"mobiletargeting:getApplicationSettings",
"mobiletargeting:getApps",
"mobiletargeting:getBaiduChannel",
```

```
"mobiletargeting:getCampaign",
"mobiletargeting:getCampaignActivities",
"mobiletargeting:getCampaigns",
"mobiletargeting:getCampaignVersion",
"mobiletargeting:getCampaignVersions",
"mobiletargeting:getEmailChannel",
"mobiletargeting:getEndpoint",
"mobiletargeting:getEventStream",
"mobiletargeting:getExportJob",
"mobiletargeting:getExportJobs",
"mobiletargeting:getGcmChannel",
"mobiletargeting:getImportJob",
"mobiletargeting:getImportJobs",
"mobiletargeting:getJourney",
"mobiletargeting:getJourneyExecutionMetrics",
"mobiletargeting:getJourneyExecutionActivityMetrics",
"mobiletargeting:getJourneyRunExecutionActivityMetrics",
"mobiletargeting:getJourneyRunExecutionMetrics",
"mobiletargeting:getJourneyRuns",
"mobiletargeting:getSegment",
"mobiletargeting:getSegmentImportJobs",
"mobiletargeting:getSegments",
"mobiletargeting:getSegmentVersion",
"mobiletargeting:getSegmentVersions",
"mobiletargeting:getSmsChannel",
"mobiletargeting:listJourneys",
"mq:describeBroker",
"mq:describeConfiguration",
"mq:describeConfigurationRevision",
"mq:describeUser",
"mq:listBrokers",
"mq:listConfigurationRevisions",
"mq:listConfigurations",
"mq:listUsers",
"m2:getApplication",
"m2:getApplicationVersion",
"m2:getBatchJobExecution",
"m2:getDataSetDetails",
"m2:getDataSetImportTask",
"m2:getDeployment",
"m2:getEnvironment",
"m2:listApplications",
"m2:listApplicationVersions",
"m2:listBatchJobDefinitions",
```

```
"m2:listBatchJobExecutions",
"m2:listDataSetImportHistory",
"m2:listDataSets",
"m2:listDeployments",
"m2:listEngineVersions",
"m2:listEnvironments",
"network-firewall:describeFirewall",
"network-firewall:describeFirewallPolicy",
"network-firewall:describeLoggingConfiguration",
"network-firewall:describeRuleGroup",
"network-firewall:describeTlsInspectionConfiguration",
"network-firewall:listFirewallPolicies",
"network-firewall:listFirewalls",
"network-firewall:listRuleGroups",
"network-firewall:listTlsInspectionConfigurations",
"networkmanager:describeGlobalNetworks",
"networkmanager:getConnectAttachment",
"networkmanager:getConnections",
"networkmanager:getConnectPeer",
"networkmanager:getConnectPeerAssociations",
"networkmanager:getCoreNetwork",
"networkmanager:getCoreNetworkChangeEvents",
"networkmanager:getCoreNetworkChangeSet",
"networkmanager:getCoreNetworkPolicy",
"networkmanager:getCustomerGatewayAssociations",
"networkmanager:getDevices",
"networkmanager:getLinkAssociations",
"networkmanager:getLinks",
"networkmanager:getNetworkResourceCounts",
"networkmanager:getNetworkResourceRelationships",
"networkmanager:getNetworkResources",
"networkmanager:getNetworkRoutes",
"networkmanager:getNetworkTelemetry",
"networkmanager:getResourcePolicy",
"networkmanager:getRouteAnalysis",
"networkmanager:getSites",
"networkmanager:getSiteToSiteVpnAttachment",
"networkmanager:getTransitGatewayConnectPeerAssociations",
"networkmanager:getTransitGatewayPeering",
"networkmanager:getTransitGatewayRegistrations",
"networkmanager:getTransitGatewayRouteTableAttachment",
"networkmanager:getVpcAttachment",
"networkmanager:listAttachments",
"networkmanager:listConnectPeers",
```

```
"networkmanager:listCoreNetworkPolicyVersions",
"networkmanager:listCoreNetworks",
"networkmanager:listOrganizationServiceAccessStatus",
"networkmanager:listPeerings",
"networkmanager:listTagsForResource",
"nimble:getEula",
"nimble:getLaunchProfile",
"nimble:getLaunchProfileDetails",
"nimble:getLaunchProfileInitialization",
"nimble:getLaunchProfileMember",
"nimble:getStreamingImage",
"nimble:getStreamingSession",
"nimble:getStreamingSessionStream",
"nimble:getStudio",
"nimble:getStudioComponent",
"nimble:listEulaAcceptances",
"nimble:listEulas",
"nimble:listLaunchProfiles",
"nimble:listStreamingImages",
"nimble:listStreamingSessions",
"nimble:listStudioComponents",
"nimble:listStudios",
"notifications:getEventRule",
"notifications:getNotificationConfiguration",
"notifications:getNotificationEvent",
"notifications:listChannels",
"notifications:listEventRules",
"notifications:listNotificationConfigurations",
"notifications:listNotificationEvents",
"notifications:listNotificationHubs",
"notifications-contacts:getEmailContact",
"notifications-contacts:listEmailContacts",
"oam:getLink",
"oam:getSink",
"oam:getSinkPolicy",
"oam:listAttachedLinks",
"oam:listLinks",
"oam:listSinks",
"omics:getAnnotationImportJob",
"omics:getAnnotationStore",
"omics:getReadSetImportJob",
"omics:getReadSetMetadata",
"omics:getReference",
"omics:getReferenceImportJob",
```

```
"omics:getReferenceMetadata",
"omics:getReferenceStore",
"omics:getRun",
"omics:getRunGroup",
"omics:getSequenceStore",
"omics:getVariantImportJob",
"omics:getVariantStore",
"omics:getWorkflow",
"omics:listAnnotationImportJobs",
"omics:listAnnotationStores",
"omics:listMultipartReadSetUploads",
"omics:listReadSetImportJobs",
"omics:listReadSets",
"omics:listReadSetUploadParts",
"omics:listReferenceImportJobs",
"omics:listReferenceStores",
"omics:listReferences",
"omics:listRunGroups",
"omics:listRunTasks",
"omics:listRuns",
"omics:listSequenceStores",
"omics:listVariantImportJobs",
"omics:listVariantStores",
"omics:listWorkflows",
"opsworks-cm:describeAccountAttributes",
"opsworks-cm:describeBackups",
"opsworks-cm:describeEvents",
"opsworks-cm:describeNodeAssociationStatus",
"opsworks-cm:describeServers",
"opsworks:describeAgentVersions",
"opsworks:describeApps",
"opsworks:describeCommands",
"opsworks:describeDeployments",
"opsworks:describeEcsClusters",
"opsworks:describeElasticIps",
"opsworks:describeElasticLoadBalancers",
"opsworks:describeInstances",
"opsworks:describeLayers",
"opsworks:describeLoadBasedAutoScaling",
"opsworks:describeMyUserProfile",
"opsworks:describePermissions",
"opsworks:describeRaidArrays",
"opsworks:describeRdsDbInstances",
"opsworks:describeServiceErrors",
```

```
"opsworks:describeStackProvisioningParameters",
"opsworks:describeStacks",
"opsworks:describeStackSummary",
"opsworks:describeTimeBasedAutoScaling",
"opsworks:describeUserProfiles",
"opsworks:describeVolumes",
"opsworks:getHostnameSuggestion",
"organizations:listAccounts",
"organizations:listTagsForResource",
"outposts:getCatalogItem",
"outposts:getConnection",
"outposts:getOrder",
"outposts:getOutpost",
"outposts:getOutpostInstanceTypes",
"outposts:getSite",
"outposts:listAssets",
"outposts:listCatalogItems",
"outposts:listOrders",
"outposts:listOutposts",
"outposts:listSites",
"personalize:describeAlgorithm",
"personalize:describeBatchInferenceJob",
"personalize:describeBatchSegmentJob",
"personalize:describeCampaign",
"personalize:describeDataset",
"personalize:describeDatasetExportJob",
"personalize:describeDatasetGroup",
"personalize:describeDatasetImportJob",
"personalize:describeEventTracker",
"personalize:describeFeatureTransformation",
"personalize:describeFilter",
"personalize:describeRecipe",
"personalize:describeRecommender",
"personalize:describeSchema",
"personalize:describeSolution",
"personalize:describeSolutionVersion",
"personalize:getPersonalizedRanking",
"personalize:getRecommendations",
"personalize:getSolutionMetrics",
"personalize:listBatchInferenceJobs",
"personalize:listBatchSegmentJobs",
"personalize:listCampaigns",
"personalize:listDatasetExportJobs",
"personalize:listDatasetGroups",
```



```
"personalize:listDatasetImportJobs",
"personalize:listDatasets",
"personalize:listEventTrackers",
"personalize:listRecipes",
"personalize:listRecommenders",
"personalize:listSchemas",
"personalize:listSolutions",
"personalize:listSolutionVersions",
"pipes:describePipe",
"pipes:listPipes",
"pipes:listTagsForResource",
"polly:describeVoices",
"polly:getLexicon",
"polly:listLexicons",
"pricing:describeServices",
"pricing:getAttributeValues",
"pricing:getProducts",
"private-networks:getDeviceIdentifier",
"private-networks:getNetwork",
"private-networks:getNetworkResource",
"private-networks:listDeviceIdentifiers",
"private-networks:listNetworks",
"private-networks:listNetworkResources",
"quicksight:describeAccountCustomization",
"quicksight:describeAccountSettings",
"quicksight:describeAccountSubscription",
"quicksight:describeAnalysis",
"quicksight:describeAnalysisPermissions",
"quicksight:describeDashboard",
"quicksight:describeDashboardPermissions",
"quicksight:describeDataSet",
"quicksight:describeDataSetPermissions",
"quicksight:describeDataSetRefreshProperties",
"quicksight:describeDataSource",
"quicksight:describeDataSourcePermissions",
"quicksight:describeFolder",
"quicksight:describeFolderPermissions",
"quicksight:describeFolderResolvedPermissions",
"quicksight:describeGroup",
"quicksight:describeGroupMembership",
"quicksight:describeIAMPolicyAssignment",
"quicksight:describeIngestion",
"quicksight:describeIpRestriction",
"quicksight:describeNamespace",
```

```
"quicksight:describeRefreshSchedule",
"quicksight:describeTemplate",
"quicksight:describeTemplateAlias",
"quicksight:describeTemplatePermissions",
"quicksight:describeTheme",
"quicksight:describeThemeAlias",
"quicksight:describeThemePermissions",
"quicksight:describeTopic",
"quicksight:describeTopicPermissions",
"quicksight:describeTopicRefresh",
"quicksight:describeTopicRefreshSchedule",
"quicksight:describeUser",
"quicksight:describeVPCConnection",
"quicksight:listAnalyses",
"quicksight:listDashboards",
"quicksight:listDashboardVersions",
"quicksight:listDataSets",
"quicksight:listDataSources",
"quicksight:listFolderMembers",
"quicksight:listFolders",
"quicksight:listGroupMemberships",
"quicksight:listGroups",
"quicksight:listIAMPolicyAssignments",
"quicksight:listIAMPolicyAssignmentsForUser",
"quicksight:listIngestions",
"quicksight:listNamespaces",
"quicksight:listRefreshSchedules",
"quicksight:listTemplateAliases",
"quicksight:listTemplates",
"quicksight:listTemplateVersions",
"quicksight:listThemeAliases",
"quicksight:listThemes",
"quicksight:listThemeVersions",
"quicksight:listTopicRefreshSchedules",
"quicksight:listTopics",
"quicksight:listUserGroups",
"quicksight:listUsers",
"quicksight:listVPCConnections",
"quicksight:searchAnalyses",
"quicksight:searchDashboards",
"quicksight:searchDataSets",
"quicksight:searchDataSources",
"quicksight:searchFolders",
"quicksight:searchGroups",
```

```
"ram:getPermission",
"ram:getResourceShareAssociations",
"ram:getResourceShareInvitations",
"ram:getResourceShares",
"ram:listPendingInvitationResources",
"ram:listPrincipals",
"ram:listResources",
"ram:listResourceSharePermissions",
"rbin:getRule",
"rbin:listRules",
"rds:describeAccountAttributes",
"rds:describeBlueGreenDeployments",
"rds:describeCertificates",
"rds:describeDBClusterEndpoints",
"rds:describeDBClusterParameterGroups",
"rds:describeDBClusterParameters",
"rds:describeDBClusters",
"rds:describeDBClusterSnapshots",
"rds:describeDBEngineVersions",
"rds:describeDBInstanceAutomatedBackups",
"rds:describeDBInstances",
"rds:describeDBLogFiles",
"rds:describeDBParameterGroups",
"rds:describeDBParameters",
"rds:describeDBSecurityGroups",
"rds:describeDBSnapshotAttributes",
"rds:describeDBSnapshots",
"rds:describeDBSubnetGroups",
"rds:describeEngineDefaultClusterParameters",
"rds:describeEngineDefaultParameters",
"rds:describeEventCategories",
"rds:describeEvents",
"rds:describeEventSubscriptions",
"rds:describeExportTasks",
"rds:describeGlobalClusters",
"rds:describeIntegrations",
"rds:describeOptionGroupOptions",
"rds:describeOptionGroups",
"rds:describeOrderableDBInstanceOptions",
"rds:describePendingMaintenanceActions",
"rds:describeReservedDBInstances",
"rds:describeReservedDBInstancesOfferings",
"rds:describeSourceRegions",
"rds:describeValidDBInstanceModifications",
```

```
"rds:listTagsForResource",
"redshift-data:describeStatement",
"redshift-data:listStatements",
"redshift:describeClusterParameterGroups",
"redshift:describeClusterParameters",
"redshift:describeClusters",
"redshift:describeClusterSecurityGroups",
"redshift:describeClusterSnapshots",
"redshift:describeClusterSubnetGroups",
"redshift:describeClusterVersions",
"redshift:describeDataShares",
"redshift:describeDataSharesForConsumer",
"redshift:describeDataSharesForProducer",
"redshift:describeDefaultClusterParameters",
"redshift:describeEventCategories",
"redshift:describeEvents",
"redshift:describeEventSubscriptions",
"redshift:describeHsmClientCertificates",
"redshift:describeHsmConfigurations",
"redshift:describeLoggingStatus",
"redshift:describeOrderableClusterOptions",
"redshift:describeReservedNodeOfferings",
"redshift:describeReservedNodes",
"redshift:describeResize",
"redshift:describeSnapshotCopyGrants",
"redshift:describeStorage",
"redshift:describeTableRestoreStatus",
"redshift:describeTags",
"redshift-serverless:getEndpointAccess",
"redshift-serverless:getNamespace",
"redshift-serverless:getRecoveryPoint",
"redshift-serverless:getSnapshot",
"redshift-serverless:getTableRestoreStatus",
"redshift-serverless:getUsageLimit",
"redshift-serverless:getWorkgroup",
"redshift-serverless:listEndpointAccess",
"redshift-serverless:listNamespaces",
"redshift-serverless:listRecoveryPoints",
"redshift-serverless:listSnapshots",
"redshift-serverless:listTableRestoreStatus",
"redshift-serverless:listUsageLimits",
"redshift-serverless:listWorkgroups",
"rekognition:listCollections",
"rekognition:listFaces",
```

```
"resource-explorer-2:getAccountLevelServiceConfiguration",
"resource-explorer-2:getIndex",
"resource-explorer-2:getView",
"resource-explorer-2:listIndexes",
"resource-explorer-2:listViews",
"resource-explorer-2:search",
"resource-groups:getGroup",
"resource-groups:getGroupQuery",
"resource-groups:getTags",
"resource-groups:listGroupResources",
"resource-groups:listGroups",
"resource-groups:searchResources",
"robomaker:batchDescribeSimulationJob",
"robomaker:describeDeploymentJob",
"robomaker:describeFleet",
"robomaker:describeRobot",
"robomaker:describeRobotApplication",
"robomaker:describeSimulationApplication",
"robomaker:describeSimulationJob",
"robomaker:listDeploymentJobs",
"robomaker:listFleets",
"robomaker:listRobotApplications",
"robomaker:listRobots",
"robomaker:listSimulationApplications",
"robomaker:listSimulationJobs",
"route53-recovery-cluster:getRoutingControlState",
"route53-recovery-cluster:listRoutingControls",
"route53-recovery-control-config:describeControlPanel",
"route53-recovery-control-config:describeRoutingControl",
"route53-recovery-control-config:describeSafetyRule",
"route53-recovery-control-config:listControlPanels",
"route53-recovery-control-config:listRoutingControls",
"route53-recovery-control-config:listSafetyRules",
"route53-recovery-readiness:getCell",
"route53-recovery-readiness:getCellReadinessSummary",
"route53-recovery-readiness:getReadinessCheck",
"route53-recovery-readiness:getReadinessCheckResourceStatus",
"route53-recovery-readiness:getReadinessCheckStatus",
"route53-recovery-readiness:getRecoveryGroup",
"route53-recovery-readiness:getRecoveryGroupReadinessSummary",
"route53-recovery-readiness:listCells",
"route53-recovery-readiness:listReadinessChecks",
"route53-recovery-readiness:listRecoveryGroups",
"route53-recovery-readiness:listResourceSets",
```

```
"route53:getAccountLimit",
"route53:getChange",
"route53:getCheckerIpRanges",
"route53:getDNSSEC",
"route53:getGeoLocation",
"route53:getHealthCheck",
"route53:getHealthCheckCount",
"route53:getHealthCheckLastFailureReason",
"route53:getHealthCheckStatus",
"route53:getHostedZone",
"route53:getHostedZoneCount",
"route53:getHostedZoneLimit",
"route53:getQueryLoggingConfig",
"route53:getReusableDelegationSet",
"route53:getTrafficPolicy",
"route53:getTrafficPolicyInstance",
"route53:getTrafficPolicyInstanceCount",
"route53:listCidrBlocks",
"route53:listCidrCollections",
"route53:listCidrLocations",
"route53:listGeoLocations",
"route53:listHealthChecks",
"route53:listHostedZones",
"route53:listHostedZonesByName",
"route53:listHostedZonesByVpc",
"route53:listQueryLoggingConfigs",
"route53:listResourceRecordSets",
"route53:listReusableDelegationSets",
"route53:listTrafficPolicies",
"route53:listTrafficPolicyInstances",
"route53:listTrafficPolicyInstancesByHostedZone",
"route53:listTrafficPolicyInstancesByPolicy",
"route53:listTrafficPolicyVersions",
"route53:listVPCAssociationAuthorizations",
"route53domains:checkDomainAvailability",
"route53domains:getContactReachabilityStatus",
"route53domains:getDomainDetail",
"route53domains:getOperationDetail",
"route53domains:listDomains",
"route53domains:listOperations",
"route53domains:listPrices",
"route53domains:listTagsForDomain",
"route53domains:viewBilling",
"route53resolver:getFirewallConfig",
```

```
"route53resolver:getFirewallDomainList",
"route53resolver:getFirewallRuleGroup",
"route53resolver:getFirewallRuleGroupAssociation",
"route53resolver:getFirewallRuleGroupPolicy",
"route53resolver:getOutpostResolver",
"route53resolver:getResolverDnssecConfig",
"route53resolver:getResolverQueryLogConfig",
"route53resolver:getResolverQueryLogConfigAssociation",
"route53resolver:getResolverQueryLogConfigPolicy",
"route53resolver:getResolverRule",
"route53resolver:getResolverRuleAssociation",
"route53resolver:getResolverRulePolicy",
"route53resolver:listFirewallConfigs",
"route53resolver:listFirewallDomainLists",
"route53resolver:listFirewallDomains",
"route53resolver:listFirewallRuleGroupAssociations",
"route53resolver:listFirewallRuleGroups",
"route53resolver:listFirewallRules",
"route53resolver:listOutpostResolvers",
"route53resolver:listResolverConfigs",
"route53resolver:listResolverDnssecConfigs",
"route53resolver:listResolverEndpointIpAddresses",
"route53resolver:listResolverEndpoints",
"route53resolver:listResolverQueryLogConfigAssociations",
"route53resolver:listResolverQueryLogConfigs",
"route53resolver:listResolverRuleAssociations",
"route53resolver:listResolverRules",
"route53resolver:listTagsForResource",
"rum:batchGetRumMetricDefinitions",
"rum:getAppMonitor",
"rum:listAppMonitors",
"rum:listRumMetricsDestinations",
"s3:describeJob",
"s3:describeMultiRegionAccessPointOperation",
"s3:getAccelerateConfiguration",
"s3:getAccessPoint",
"s3:getAccessPointConfigurationForObjectLambda",
"s3:getAccessPointForObjectLambda",
"s3:getAccessPointPolicy",
"s3:getAccessPointPolicyForObjectLambda",
"s3:getAccessPointPolicyStatus",
"s3:getAccessPointPolicyStatusForObjectLambda",
"s3:getAccountPublicAccessBlock",
"s3:getAnalyticsConfiguration",
```

```
"s3:getBucketAcl",
"s3:getBucketCORS",
"s3:getBucketLocation",
"s3:getBucketLogging",
"s3:getBucketNotification",
"s3:getBucketObjectLockConfiguration",
"s3:getBucketOwnershipControls",
"s3:getBucketPolicy",
"s3:getBucketPolicyStatus",
"s3:getBucketPublicAccessBlock",
"s3:getBucketRequestPayment",
"s3:getBucketVersioning",
"s3:getBucketWebsite",
"s3:getEncryptionConfiguration",
"s3:getIntelligentTieringConfiguration",
"s3:getInventoryConfiguration",
"s3:getLifecycleConfiguration",
"s3:getMetricsConfiguration",
"s3:getMultiRegionAccessPoint",
"s3:getMultiRegionAccessPointPolicy",
"s3:getMultiRegionAccessPointPolicyStatus",
"s3:getMultiRegionAccessPointRoutes",
"s3:getObjectLegalHold",
"s3:getObjectRetention",
"s3:getReplicationConfiguration",
"s3:getStorageLensConfiguration",
"s3:listAccessPoints",
"s3:listAccessPointsForObjectLambda",
"s3:listAllMyBuckets",
"s3:listBucket",
"s3:listBucketMultipartUploads",
"s3:listBucketVersions",
"s3:listJobs",
"s3:listMultipartUploadParts",
"s3:listMultiRegionAccessPoints",
"s3:listStorageLensConfigurations",
"s3express:listAllMyDirectoryBuckets",
"sagemaker:describeAction",
"sagemaker:describeAlgorithm",
"sagemaker:describeApp",
"sagemaker:describeAppImageConfig",
"sagemaker:describeArtifact",
"sagemaker:describeAutoMLJob",
"sagemaker:describeCodeRepository",
```



```
"sagemaker:describeCompilationJob",
"sagemaker:describeContext",
"sagemaker:describeDataQualityJobDefinition",
"sagemaker:describeDevice",
"sagemaker:describeDeviceFleet",
"sagemaker:describeDomain",
"sagemaker:describeEdgeDeploymentPlan",
"sagemaker:describeEdgePackagingJob",
"sagemaker:describeEndpoint",
"sagemaker:describeEndpointConfig",
"sagemaker:describeExperiment",
"sagemaker:describeFeatureGroup",
"sagemaker:describeFeatureMetadata",
"sagemaker:describeFlowDefinition",
"sagemaker:describeHub",
"sagemaker:describeHubContent",
"sagemaker:describeHumanTaskUi",
"sagemaker:describeHyperParameterTuningJob",
"sagemaker:describeImage",
"sagemaker:describeImageVersion",
"sagemaker:describeInferenceExperiment",
"sagemaker:describeInferenceRecommendationsJob",
"sagemaker:describeLabelingJob",
"sagemaker:describeModel",
"sagemaker:describeModelBiasJobDefinition",
"sagemaker:describeModelCard",
"sagemaker:describeModelCardExportJob",
"sagemaker:describeModelExplainabilityJobDefinition",
"sagemaker:describeModelPackage",
"sagemaker:describeModelPackageGroup",
"sagemaker:describeModelQualityJobDefinition",
"sagemaker:describeMonitoringSchedule",
"sagemaker:describeNotebookInstance",
"sagemaker:describeNotebookInstanceLifecycleConfig",
"sagemaker:describePipeline",
"sagemaker:describePipelineDefinitionForExecution",
"sagemaker:describePipelineExecution",
"sagemaker:describeProcessingJob",
"sagemaker:describeProject",
"sagemaker:describeSpace",
"sagemaker:describeStudioLifecycleConfig",
"sagemaker:describeSubscribedWorkteam",
"sagemaker:describeTrainingJob",
"sagemaker:describeTransformJob",
```

```
"sagemaker:describeTrial",
"sagemaker:describeTrialComponent",
"sagemaker:describeUserProfile",
"sagemaker:describeWorkforce",
"sagemaker:describeWorkteam",
"sagemaker:getDeviceFleetReport",
"sagemaker:getModelPackageGroupPolicy",
"sagemaker:getSagemakerServicecatalogPortfolioStatus",
"sagemaker:listActions",
"sagemaker:listAlgorithms",
"sagemaker:listAliases",
"sagemaker:listAppImageConfigs",
"sagemaker:listApps",
"sagemaker:listArtifacts",
"sagemaker:listAssociations",
"sagemaker:listAutoMLJobs",
"sagemaker:listCandidatesForAutoMLJob",
"sagemaker:listCodeRepositories",
"sagemaker:listCompilationJobs",
"sagemaker:listContexts",
"sagemaker:listDataQualityJobDefinitions",
"sagemaker:listDeviceFleets",
"sagemaker:listDevices",
"sagemaker:listDomains",
"sagemaker:listEdgeDeploymentPlans",
"sagemaker:listEdgePackagingJobs",
"sagemaker:listEndpointConfigs",
"sagemaker:listEndpoints",
"sagemaker:listExperiments",
"sagemaker:listFeatureGroups",
"sagemaker:listFlowDefinitions",
"sagemaker:listHubContents",
"sagemaker:listHubContentVersions",
"sagemaker:listHubs",
"sagemaker:listHumanTaskUis",
"sagemaker:listHyperParameterTuningJobs",
"sagemaker:listImages",
"sagemaker:listImageVersions",
"sagemaker:listInferenceExperiments",
"sagemaker:listInferenceRecommendationsJobs",
"sagemaker:listInferenceRecommendationsJobSteps",
"sagemaker:listLabelingJobs",
"sagemaker:listLabelingJobsForWorkteam",
"sagemaker:listLineageGroups",
```

```
"sagemaker:listModelBiasJobDefinitions",
"sagemaker:listModelCardExportJobs",
"sagemaker:listModelCards",
"sagemaker:listModelCardVersions",
"sagemaker:listModelExplainabilityJobDefinitions",
"sagemaker:listModelMetadata",
"sagemaker:listModelPackageGroups",
"sagemaker:listModelPackages",
"sagemaker:listModelQualityJobDefinitions",
"sagemaker:listModels",
"sagemaker:listMonitoringAlertHistory",
"sagemaker:listMonitoringAlerts",
"sagemaker:listMonitoringExecutions",
"sagemaker:listMonitoringSchedules",
"sagemaker:listNotebookInstanceLifecycleConfigs",
"sagemaker:listNotebookInstances",
"sagemaker:listPipelineExecutions",
"sagemaker:listPipelineExecutionSteps",
"sagemaker:listPipelineParametersForExecution",
"sagemaker:listPipelines",
"sagemaker:listProcessingJobs",
"sagemaker:listProjects",
"sagemaker:listSpaces",
"sagemaker:listStageDevices",
"sagemaker:listStudioLifecycleConfigs",
"sagemaker:listSubscribedWorkteams",
"sagemaker:listTags",
"sagemaker:listTrainingJobs",
"sagemaker:listTrainingJobsForHyperParameterTuningJob",
"sagemaker:listTransformJobs",
"sagemaker:listTrialComponents",
"sagemaker:listTrials",
"sagemaker:listUserProfile",
"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"
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSystemsManagerAccountDiscoveryServicePolicy

AWSSystemsManagerAccountDiscoveryServicePolicy es una [política administrada por AWS](#) que: concede a AWS Systems Manager (SSM) permiso para descubrir la información de la Cuenta de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de octubre de 2019 a las 17:21 UTC
- Hora de edición: 17 de octubre de 2022 a las 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSystemsManagerChangeManagementServicePolicy

AWSSystemsManagerChangeManagementServicePolicy es una [política administrada por AWS](#) que: proporciona acceso a los recursos de AWS gestionados o utilizados por el marco de gestión de cambios de AWS Systems Manager.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de diciembre de 2020 a las 22:21 UTC
- Hora de edición: 7 de diciembre de 2020 a las 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm>DeleteAssociation",
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:GetCalendarState",
        "ssm:GetDocument"
      ]
    }
  ],
}
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sso:ListDirectoryAssociations"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sso-directory:DescribeUsers",
      "sso-directory:IsMemberInGroup"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:GetGroup",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
```

```
        "ssm.amazonaws.com"
      ]
    }
  }
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSystemsManagerForSAPFullAccess

AWSSystemsManagerForSAPFullAccess es una [política administrada por AWS](#) que: otorga acceso total al servicio de AWS Systems Manager para SAP

Uso de la política

Puede asociar AWSSystemsManagerForSAPFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de noviembre de 2022 a las 02:11 UTC
- Hora de edición: 18 de noviembre de 2022 a las 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSystemsManagerForSAPReadOnlyAccess

AWSSystemsManagerForSAPReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio de AWS Systems Manager para SAP

Uso de la política

Puede asociar AWSSystemsManagerForSAPReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 17 de noviembre de 2022 a las 02:11 UTC
- Hora de edición: 17 de noviembre de 2022 a las 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

AWSSystemsManagerOpsDataSyncServiceRolePolicy es una [política administrada por AWS](#) que: permite que el rol de IAM para SSM Explorer gestione las operaciones relacionadas con OpsData

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de abril de 2021 a las 20:42 UTC
- Hora de edición: 28 de junio de 2023 a las 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    }
  ],
}
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "securityhub:GetFindings",
    "securityhub:BatchUpdateFindings"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Confidence" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Criticality" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
```

```
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/Note.Text" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/RelatedFindings" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/Types" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
      }
    }
  }
}
```

```
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/VerificationState" : false
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSThinkboxAssetServerPolicy

AWSThinkboxAssetServerPolicy es una [política administrada por AWS](#) que otorga al Portal Asset Server de AWS los permisos necesarios para que funcione con normalidad.

Uso de la política

Puede asociar AWSThinkboxAssetServerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2020 a las 19:18 UTC
- Hora de edición: 27 de mayo de 2020 a las 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    }
  ]
}
```

```
]
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSThinkboxAWSPortalAdminPolicy

AWSThinkboxAWSPortalAdminPolicy es una [política AWS gestionada](#) que: esta política otorga al software Deadline de AWS Thinkbox acceso total a varios AWS servicios necesarios para la administración AWS del portal. Esto incluye el acceso para crear etiquetas arbitrarias en varios tipos de recursos de EC2.

Uso de la política

Puede asociar AWSThinkboxAWSPortalAdminPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:41 UTC
- Hora editada: 23 de febrero de 2024 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
```

```

    "ec2:DescribeInstanceTypeOfferings",
    "ec2:DescribeRegions",
    "ec2:DescribeSpotFleetRequestHistory",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSpotFleetInstances",
    "ec2:DescribeSpotFleetRequests",
    "ec2:DescribeSpotPriceHistory",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:GetConsoleOutput",
    "ec2:ImportKeyPair",
    "ec2:ReleaseAddress",
    "ec2:RequestSpotFleet",
    "ec2:CancelSpotFleetRequests",
    "ec2:DisassociateAddress",
    "ec2>DeleteFleets",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteVpc",
    "ec2>DeletePlacementGroup",
    "ec2>DeleteVpcEndpoints",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteRoute",
    "ec2>DeleteRouteTable",
    "ec2:DisassociateRouteTable",
    "ec2>DeleteSubnet",
    "ec2>DeleteNatGateway",
    "ec2:DetachInternetGateway",
    "ec2:ModifyInstanceAttribute",
    "ec2:ModifyFleet",
    "ec2:ModifySpotFleetRequest",
    "ec2:ModifyVpcAttribute"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal2",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:key-pair/*",

```

```

    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:image/*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal3",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "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" : "AWSThinkboxAWSPortal17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal18",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal19",
  "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*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSThinkboxAWSPortalGatewayPolicy

AWSThinkboxAWSPortalGatewayPolicy es una [política administrada por AWS](#) que: concede al equipo de la Puerta de enlace de almacenamiento de AWS los permisos necesarios para funcione con formalidad.

Uso de la política

Puede asociar AWSThinkboxAWSPortalGatewayPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2020 a las 19:05 UTC
- Hora de edición: 30 de junio de 2020 a las 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
    "logs:CreateLogStream"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/thinkbox*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-portal-cache*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "dynamodb:Scan",
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::stack*"
  ]
},
{
```

```
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::stack*/gateway_certs/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSThinkboxAWSPortalWorkerPolicy

AWSThinkboxAWSPortalWorkerPolicy es una [política administrada por AWS](#) que: concede a Deadline Workers del Portal de AWS los permisos necesarios para el funcionamiento normal.

Uso de la política

Puede asociar AWSThinkboxAWSPortalWorkerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2020 a las 19:15 UTC
- Hora de edición: 7 de diciembre de 2020 a las 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-portal-cache*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::stack*/gateway_certs/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/thinkbox*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "*"
  ]
},
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "sqs:SendMessage",
    "sqs:GetQueueUrl"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:DeadlineAWS*"
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

AWSThinkboxDeadlineResourceTrackerAccessPolicy es una [política administrada por AWS](#) que: concede los permisos necesarios para el funcionamiento del Deadline Resource Tracker de Thinkbox de AWS. Esto incluye el acceso total a algunas acciones de EC2, como DeleteFleets y CancelSpotFleetRequests.

Uso de la política

Puede asociar AWSThinkboxDeadlineResourceTrackerAccessPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2020 a las 19:25 UTC

- Hora de edición: 27 de mayo de 2020 a las 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb>DeleteItem",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:PutItem",
        "dynamodb:Scan",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable"
      ],
    },
  ],
}
```

```

    "Resource" : [
      "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
      "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
      "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CancelSpotFleetRequests",
      "ec2>DeleteFleets",
      "ec2:DescribeFleetInstances",
      "ec2:DescribeFleets",
      "ec2:DescribeInstances",
      "ec2:DescribeSpotFleetInstances",
      "ec2:DescribeSpotFleetRequests"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RebootInstances",
      "ec2:TerminateInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:PutEvents"
    ],
    "Resource" : [
      "arn:aws:events:*:*:event-bus/default"
    ]
  }

```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:DeleteMessage",
      "sqs:GetQueueAttributes",
      "sqs:ReceiveMessage"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
    ]
  }
]
```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

AWSThinkboxDeadlineResourceTrackerAdminPolicy es una [política administrada por AWS](#) que: concede los permisos necesarios para crear, destruir y administrar el Deadline Resource Tracker de Thinkbox de AWS.

Uso de la política

Puede asociar AWSThinkboxDeadlineResourceTrackerAdminPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2020 a las 19:29 UTC
- Hora de edición: 22 de junio de 2022 a las 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

AWSThinkboxDeadlineSpotEventPluginAdminPolicy es una [política administrada por AWS](#) que: concede los permisos necesarios para el complemento Deadline Spot Event de Thinkbox de AWS. Esto incluye el permiso para solicitar, modificar y cancelar una flota de spot, y el permiso limitado de PassRole.

Uso de la política

Puede asociar AWSThinkboxDeadlineSpotEventPluginAdminPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2020 a las 19:38 UTC
- Hora de edición: 27 de mayo de 2020 a las 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```



```
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/aws-service-role/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com"
      ]
    }
  }
}
```

```

    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam::*:instance-profile/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
}

```

```
    }  
  }  
} ]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy es una [política administrada por AWS](#) que: concede los permisos necesarios para que una instancia EC2 ejecute el software AWS Thinkbox Deadline Spot Event Plugin Worker.

Uso de la política

Puede asociar AWSThinkboxDeadlineSpotEventPluginWorkerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de mayo de 2020 a las 19:35 UTC
- Hora de edición: 7 de diciembre de 2020 a las 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
        "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "sqs:GetQueueUrl",
        "sqs:SendMessage"
    ],
    "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
    ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSTransferConsoleFullAccess

AWSTransferConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Transfer de AWS por medio de la AWS Management Console

Uso de la política

Puede asociar AWSTransferConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de diciembre de 2020 a las 19:33 UTC

- Hora de edición: 14 de diciembre de 2020 a las 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "health:DescribeEventAggregates",
        "iam:GetPolicyVersion",
        "iam:ListPolicies",
        "iam:ListRoles",

```

```
        "route53:ListHostedZones",
        "s3:ListAllMyBuckets",
        "transfer:*"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSTransferFullAccess

AWSTransferFullAccess es una [política administrada por AWS](#) que: concede acceso total al servicio de Transfer de AWS.

Uso de la política

Puede asociar AWSTransferFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de diciembre de 2020 a las 19:37 UTC
- Hora de edición: 14 de diciembre de 2020 a las 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "transfer:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSTransferLoggingAccess

AWSTransferLoggingAccess es una [política administrada por AWS](#) que: permite a Transfer de AWS tener acceso total a la creación de flujos y grupos de registros y guardar los eventos de registro en su cuenta

Uso de la política

Puede asociar AWSTransferLoggingAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de enero de 2019 a las 15:32 UTC
- Hora de edición: 14 de enero de 2019 a las 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSTransferReadOnlyAccess

AWSTransferReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a los servicios de Transfer de AWS.

Uso de la política

Puede asociar AWSTransferReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de agosto de 2020 a las 17:54 UTC
- Hora de edición: 27 de agosto de 2020 a las 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSTrustedAdvisorPriorityFullAccess

AWSTrustedAdvisorPriorityFullAccess es una [política administrada por AWS](#) que: otorga acceso total a Trusted Advisor Priority de AWS. Esta política también permite que el usuario agregue Trusted Advisor como servicio de confianza con AWS Organizations, y para especificar las cuentas de administrador delegadas para Trusted Advisor Priority.

Uso de la política

Puede asociar `AWSTrustedAdvisorPriorityFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 16 de agosto de 2022 a las 16:08 UTC
- Hora de edición: 16 de agosto de 2022 a las 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:UpdateRiskStatus",
        "trustedadvisor:DescribeNotificationConfigurations",
        "trustedadvisor:UpdateNotificationConfigurations",
        "trustedadvisor>DeleteNotificationConfigurationForDelegatedAdmin",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource" : "*"
    }
  ],
  {
```

```

    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators",
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "reporting.trustedadvisor.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource" : "arn:aws:organizations::*:*:*",
    "Condition" : {
      "StringEquals" : {

```

```
        "organizations:ServicePrincipal" : [  
            "reporting.trustedadvisor.amazonaws.com"  
        ]  
    }  
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

AWSTrustedAdvisorPriorityReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Trusted Advisor Priority de AWS. Esto incluye el permiso para ver las cuentas de administrador delegadas.

Uso de la política

Puede asociar AWSTrustedAdvisorPriorityReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 16 de agosto de 2022 a las 16:35 UTC
- Hora de edición: 16 de agosto de 2022 a las 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:DescribeNotificationConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
}
  }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSTrustedAdvisorReportingServiceRolePolicy

AWSTrustedAdvisorReportingServiceRolePolicy es una [política administrada por AWS](#) que: es una Política de servicio para la generación de informes de cuentas múltiples de Trusted Advisor

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de noviembre de 2019 a las 17:41 UTC
- Hora de edición: 28 de febrero de 2023 a las 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSTrustedAdvisorServiceRolePolicy

AWSTrustedAdvisorServiceRolePolicy es una [política administrada por AWS](#) que: concede acceso al servicio Trusted Advisor de AWS para ayudar a reducir costos, aumentar el rendimiento y mejorar la seguridad del entorno de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de febrero de 2018 a las 21:24 UTC
- Hora editada: 18 de enero de 2024, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Versión de la política

Versión de la política: v12 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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" : "*"

```

```
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSUserNotificationsServiceLinkedRolePolicy

AWSUserNotificationsServiceLinkedRolePolicy es una [política administrada por AWS](#) que: permite que las notificaciones de usuario de AWS llamen a los servicios de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de abril de 2023 a las 13:28 UTC
- Hora de edición: 19 de abril de 2023 a las 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events>DeleteRule",
        "events>ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSVendorInsightsAssessorFullAccess

AWSVendorInsightsAssessorFullAccess es una [política administrada por AWS](#) que: brinda acceso total para ver los recursos titulados Vendor Insights y gestionar las suscripciones a Vendor Insights

Uso de la política

Puede asociar AWSVendorInsightsAssessorFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de julio de 2022 a las 15:05 UTC
- Hora de edición: 1 de diciembre de 2022 a las 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ]
    }
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:CreateAgreementRequest",
      "aws-marketplace:GetAgreementRequest",
      "aws-marketplace:AcceptAgreementRequest",
      "aws-marketplace:CancelAgreementRequest",
      "aws-marketplace:ListAgreementRequests",
      "aws-marketplace:SearchAgreements",
      "aws-marketplace:CancelAgreement"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "artifact:GetReport",
      "artifact:GetReportMetadata",
      "artifact:GetTermForReport",
      "artifact:ListReports"
    ],
    "Resource" : "arn:aws:artifact:*::report/*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSVendorInsightsAssessorReadOnly

AWSVendorInsightsAssessorReadOnly es una [política administrada por AWS](#) que: otorga acceso de solo lectura para ver los recursos autorizados de Vendor Insights

Uso de la política

Puede asociar AWSVendorInsightsAssessorReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de julio de 2022 a las 15:05 UTC
- Hora de edición: 1 de diciembre de 2022 a las 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "artifact:GetReport",
    "artifact:GetReportMetadata",
    "artifact:GetTermForReport",
    "artifact:ListReports"
  ],
  "Resource" : "arn:aws:artifact::*:report/*"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSVendorInsightsVendorFullAccess

AWSVendorInsightsVendorFullAccess es una [política administrada por AWS](#) que: proporciona acceso total para crear y gestionar los recursos de Vendor Insights

Uso de la política

Puede asociar AWSVendorInsightsVendorFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de julio de 2022 a las 15:05 UTC
- Hora de edición: 19 de octubre de 2023 a las 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/*SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:CreateDataSource",
        "vendor-insights:UpdateDataSource",
        "vendor-insights>DeleteDataSource",
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:CreateSecurityProfile",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:AssociateDataSource",
        "vendor-insights:DisassociateDataSource",
        "vendor-insights:UpdateSecurityProfile",
        "vendor-insights:ActivateSecurityProfile",
        "vendor-insights:DeactivateSecurityProfile",
        "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
        "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:GetSecurityProfileSnapshot",

```

```

    "vendor-insights:TagResource",
    "vendor-insights:UntagResource",
    "vendor-insights:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:AcceptAgreementApprovalRequest",
    "aws-marketplace:RejectAgreementApprovalRequest",
    "aws-marketplace:GetAgreementApprovalRequest",
    "aws-marketplace:ListAgreementApprovalRequests",
    "aws-marketplace:CancelAgreement",
    "aws-marketplace:SearchAgreements"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "artifact:GetReport",
    "artifact:GetReportMetadata",
    "artifact:GetTermForReport",
    "artifact:ListReports"
  ],
  "Resource" : "arn:aws:artifact:*::report/*"
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSVendorInsightsVendorReadOnly

AWSVendorInsightsVendorReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura para ver los recursos de Vendor Insights

Uso de la política

Puede asociar AWSVendorInsightsVendorReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 26 de julio de 2022 a las 15:05 UTC
- Hora de edición: 1 de diciembre de 2022 a las 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : "aws-marketplace:ListEntities",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "vendor-insights:GetDataSource",
    "vendor-insights:ListDataSources",
    "vendor-insights:ListSecurityProfiles",
    "vendor-insights:GetSecurityProfile",
    "vendor-insights:GetSecurityProfileSnapshot",
    "vendor-insights:ListSecurityProfileSnapshots",
    "vendor-insights:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "artifact:GetReport",
    "artifact:GetReportMetadata",
    "artifact:GetTermForReport",
    "artifact:ListReports"
  ],
  "Resource" : "arn:aws:artifact:*::report/*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSVpcLatticeServiceRolePolicy

AWSVpcLatticeServiceRolePolicy es una [política administrada por AWS](#) que: permite a VPC Lattice acceder a los recursos de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2022 a las 20:47 UTC
- Hora de edición: 30 de noviembre de 2022 a las 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    }  
  }  
} ]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSVPCS2SVpnServiceRolePolicy

AWSVPCS2SVpnServiceRolePolicy es una [política administrada por AWS](#) que: permite que Site-to-Site VPN cree y gestione recursos relacionados con las conexiones del VPN.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de agosto de 2019 a las 14:13 UTC
- Hora de edición: 6 de agosto de 2019 a las 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSVPCTransitGatewayServiceRolePolicy

AWSVPCTransitGatewayServiceRolePolicy es una [política administrada por AWS](#) que permite que la Puerta de enlace de VPC Transit cree y gestione los recursos necesarios para los adjuntos de la Puerta de enlace de VPC de Transit.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 26 de noviembre de 2018 a las 16:21 UTC
- Hora de edición: 15 de abril de 2021 a las 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AssignIpv6Addresses",
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Sid" : "0"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSVPCVerifiedAccessServiceRolePolicy

AWSVPCVerifiedAccessServiceRolePolicy es una [política administrada por AWS](#) que permite que el Servicio de acceso verificado de AWS aprovisiona puntos de conexión en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2022 a las 03:35 UTC
- Hora editada: 17 de noviembre de 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/VerifiedAccessManaged" : "true"
      }
    }
  },
  {
    "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*"
  },
  {
    "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/VerifiedAccessManaged" : "true"
      }
    }
  },
  {
    "Sid" : "VerifiedAccessRoleTaggingActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
  },
```

```
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSWAFConsoleFullAccess

AWSWAFConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a AWS WAF a través de la AWS Management Console. Tenga en cuenta que esta política también otorga permisos para enumerar y actualizar las distribuciones de Amazon CloudFront. A su vez, concede permisos para ver los equilibradores de carga en AWS Elastic Load Balancing, permisos para ver las API y etapas de REST de Amazon API Gateway. Por último, brinda permisos para enumerar y ver las métricas de Amazon CloudWatch y para ver las regiones habilitadas en la cuenta.

Uso de la política

Puede asociar AWSWAFConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de abril de 2020 a las 18:38 UTC
- Hora de edición: 5 de junio de 2023 a las 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    }  
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSWAFConsoleReadOnlyAccess

`AWSWAFConsoleReadOnlyAccess` es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a AWS WAF a través de la AWS Management Console. Tenga en cuenta que esta política también otorga permisos para enumerar las distribuciones de Amazon CloudFront. A su vez, concede permisos para ver los equilibradores de carga en AWS Elastic Load Balancing, permisos para ver las API y etapas de REST de Amazon API Gateway. Por último, brinda permisos para enumerar y ver las métricas de Amazon CloudWatch y para ver las regiones habilitadas en la cuenta.

Uso de la política

Puede asociar `AWSWAFConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de abril de 2020 a las 18:43 UTC
- Hora de edición: 5 de junio de 2023 a las 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSWAFFullAccess

AWSWAFFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a las acciones de AWS WAF.

Uso de la política

Puede asociar AWSWAFFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de octubre de 2015 a las 20:44 UTC
- Hora de edición: 5 de junio de 2023 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSWAFReadOnlyAccess

AWSWAFReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a todas las acciones de AWS WAF.

Uso de la política

Puede asociar AWSWAFReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de octubre de 2015 a las 20:43 UTC
- Hora de edición: 5 de junio de 2023 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

AWSWellArchitectedDiscoveryServiceRolePolicy es una [política administrada por AWS](#) que: permite que WellArchitected acceda a los servicios y recursos de AWS relacionados con los recursos de WellArchitected en nombre de los clientes.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de abril de 2023 a las 18:36 UTC
- Hora de edición: 26 de abril de 2023 a las 18:36 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
```

```

    "servicecatalog:GetApplication",
    "servicecatalog:CreateAttributeGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:AssociateAttributeGroup",
    "servicecatalog:DisassociateAttributeGroup"
  ],
  "Resource" : [
    "arn:*:servicecatalog:*:*/applications/*",
    "arn:*:servicecatalog:*:*/attribute-groups/AWS_WellArchitected-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:UpdateAttributeGroup",
    "servicecatalog>DeleteAttributeGroup"
  ],
  "Resource" : [
    "arn:*:servicecatalog:*:*/attribute-groups/AWS_WellArchitected-*"
  ]
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

AWSWellArchitectedOrganizationsServiceRolePolicy es una [política administrada por AWS](#) que: permite que Well-Architected acceda a Organizations en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de junio de 2022 a las 17:15 UTC
- Hora de edición: 25 de julio de 2022 a las 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSWickrFullAccess

AWSWickrFullAccess es una [política administrada por AWS](#) que: concede permisos administrativos totales al servicio de Wickr, incluidas las funciones administrativas de Wickr contempladas en la AWS Management Console.

Uso de la política

Puede asociar AWSWickrFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2022 a las 20:36 UTC
- Hora de edición: 27 de noviembre de 2022 a las 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSXrayCrossAccountSharingConfiguration

AWSXrayCrossAccountSharingConfiguration es una [política administrada por AWS](#) que: proporciona capacidades para gestionar los enlaces de Observability Access Manager y establecer el intercambio de trazas de X-Ray

Uso de la política

Puede asociar AWSXrayCrossAccountSharingConfiguration a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2022 a las 13:46 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam>DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSXRayDaemonWriteAccess

AWSXRayDaemonWriteAccesses una [política AWS gestionada](#) que: permite al Daemon de AWS X-Ray retransmitir datos de segmentos de rastreo sin procesar a la API del servicio y recuperar datos de muestreo (reglas, objetivos, etc.) para que los utilice el SDK de X-Ray.

Uso de la política

Puede asociar `AWSXRayDaemonWriteAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de agosto de 2018 a las 23:00 UTC
- Hora editada: 13 de febrero de 2024 a las 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSXrayFullAccess

AWSXrayFullAccess es una [política administrada por AWS](#) que: otorga acceso total a X-Ray de AWS

Uso de la política

Puede asociar AWSXrayFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2016 a las 18:30 UTC
- Hora de edición: 1 de diciembre de 2016 a las 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSXrayReadOnlyAccess

AWSXrayReadOnlyAccesses una [política AWS gestionada que: Política gestionada](#) de solo lectura de AWS X-Ray

Uso de la política

Puede asociar AWSXrayReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2016 a las 18:27 UTC
- Hora editada: 14 de febrero de 2024 a las 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
```



```

    "xray:BatchGetTraces",
    "xray:BatchGetTraceSummaryById",
    "xray:GetDistinctTraceGraphs",
    "xray:GetServiceGraph",
    "xray:GetTraceGraph",
    "xray:GetTraceSummaries",
    "xray:GetGroups",
    "xray:GetGroup",
    "xray:ListTagsForResource",
    "xray:ListResourcePolicies",
    "xray:GetTimeSeriesServiceStatistics",
    "xray:GetInsightSummaries",
    "xray:GetInsight",
    "xray:GetInsightEvents",
    "xray:GetInsightImpactGraph"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

AWSXrayWriteOnlyAccess

AWSXrayWriteOnlyAccess es una [política administrada por AWS](#) que: es una política de solo escritura de X-Ray de AWS

Uso de la política

Puede asociar AWSXrayWriteOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2016 a las 18:19 UTC
- Hora de edición: 28 de agosto de 2018 a las 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

AWSZonalAutoshiftPracticeRunSLRPolicy es una [política AWS gestionada](#) que: proporciona acceso administrativo a las prácticas de turno zonal de ARC y acceso a los estados de CloudWatch alarma para supervisar las prácticas.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2023 a las 17:34 UTC
- Hora editada: 29 de noviembre de 2023 a las 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

BatchServiceRolePolicy

BatchServiceRolePolicy es una [política administrada por AWS](#) que: proporciona acceso al servicio Batch de AWS para gestionar los recursos necesarios, incluidos los recursos de Amazon EC2 y Amazon ECS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de marzo de 2021 a las 06:55 UTC
- Hora editada: 5 de diciembre de 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
```

```

    "ec2:DescribeSpotFleetRequests",
    "ec2:DescribeSpotPriceHistory",
    "ec2:DescribeSpotFleetRequestHistory",
    "ec2:DescribeVpcClassicLink",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:RequestSpotFleet",
    "autoscaling:DescribeAccountLimits",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeScalingActivities",
    "eks:DescribeCluster",
    "ecs:DescribeClusters",
    "ecs:DescribeContainerInstances",
    "ecs:DescribeTaskDefinition",
    "ecs:DescribeTasks",
    "ecs:ListClusters",
    "ecs:ListContainerInstances",
    "ecs:ListTaskDefinitionFamilies",
    "ecs:ListTaskDefinitions",
    "ecs:ListTasks",
    "ecs:DeregisterTaskDefinition",
    "ecs:TagResource",
    "ecs:ListAccountSettings",
    "logs:DescribeLogGroups",
    "iam:GetInstanceProfile",
    "iam:GetRole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSBatchPolicyStatement2",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
},
{
  "Sid" : "AWSBatchPolicyStatement3",
  "Effect" : "Allow",
  "Action" : [
    "logs:PutLogEvents"
  ]
}

```

```
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
  },
  {
    "Sid" : "AWSBatchPolicyStatement4",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CreateOrUpdateTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSBatchServiceTag" : "false"
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement5",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn",
          "ecs-tasks.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement6",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "spot.amazonaws.com",
          "spotfleet.amazonaws.com",
          "autoscaling.amazonaws.com",
```

```
        "ecs.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement7",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSBatchServiceTag" : "false"
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement8",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:CancelSpotFleetRequests",
      "ec2:ModifySpotFleetRequest",
      "ec2>DeleteLaunchTemplate"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSBatchServiceTag" : "false"
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement9",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling>DeleteLaunchConfiguration"
    ],
    "Resource" :
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
  },
}
```



```
{
  "Sid" : "AWSBatchPolicyStatement10",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:SetDesiredCapacity",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling:SuspendProcesses",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:TerminateInstanceInAutoScalingGroup"
  ],
  "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
},
{
  "Sid" : "AWSBatchPolicyStatement11",
  "Effect" : "Allow",
  "Action" : [
    "ecs>DeleteCluster",
    "ecs:DeregisterContainerInstance",
    "ecs:RunTask",
    "ecs:StartTask",
    "ecs:StopTask"
  ],
  "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
},
{
  "Sid" : "AWSBatchPolicyStatement12",
  "Effect" : "Allow",
  "Action" : [
    "ecs:RunTask",
    "ecs:StartTask",
    "ecs:StopTask"
  ],
  "Resource" : "arn:aws:ecs:*:*:task-definition/*"
},
{
  "Sid" : "AWSBatchPolicyStatement13",
  "Effect" : "Allow",
  "Action" : [
    "ecs:StopTask"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
```

```
},
{
  "Sid" : "AWSBatchPolicyStatement14",
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:RegisterTaskDefinition"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSBatchServiceTag" : "false"
    }
  }
},
{
  "Sid" : "AWSBatchPolicyStatement15",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:capacity-reservation/*",
    "arn:aws:ec2:*:*:elastic-gpu/*",
    "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
    "arn:aws:resource-groups:*:*:group/*"
  ]
},
{
  "Sid" : "AWSBatchPolicyStatement16",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSBatchServiceTag" : "false"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement17",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "RunInstances",
          "CreateLaunchTemplate",
          "RequestSpotFleet"
        ]
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

Billing

Billing es una [política administrada por AWS](#) que: otorga permisos para la facturación y la administración de costos. Esto incluye ver el uso de la cuenta, modificar los presupuestos y los métodos de pago.

Uso de la política

Puede asociar Billing a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:33 UTC
- Hora editada: 17 de enero de 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CertificateManagerServiceRolePolicy

CertificateManagerServiceRolePolicy es una [política administrada por AWS](#) que: es una Política de rol de servicio de Amazon Certificate Manager

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de junio de 2020 a las 17:56 UTC
- Hora de edición: 25 de junio de 2020 a las 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ClientVPNServiceConnectionsRolePolicy

ClientVPNServiceConnectionsRolePolicy es una [política administrada por AWS](#) que: permite que AWS Client VPN administre sus conexiones de punto de conexión de Client VPN.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de agosto de 2020 a las 19:48 UTC
- Hora de edición: 12 de agosto de 2020 a las 19:48 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ClientVPNServiceRolePolicy

ClientVPNServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Client VPN administre sus puntos de conexión de Client VPN.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de diciembre de 2018 a las 21:20 UTC
- Hora de edición: 12 de agosto de 2020 a las 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ds:AuthorizeApplication",
        "ds:DescribeDirectories",
```

```
    "ds:GetDirectoryLimits",
    "ds:UnauthorizeApplication",
    "logs:DescribeLogStreams",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogGroups",
    "acm:GetCertificate",
    "acm:DescribeCertificate",
    "iam:GetSAMLProvider",
    "lambda:GetFunctionConfiguration"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

CloudFormationStackSetsOrgAdminServiceRolePolicy es una [política administrada por AWS](#) que: otorga un rol de servicio para CloudFormation StackSets (cuenta maestra de Organization)

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de diciembre de 2019 a las 00:20 UTC
- Hora de edición: 10 de diciembre de 2019 a las 00:20 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsAWSOrganizationsReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRoleInMemberAccounts",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

CloudFormationStackSetsOrgMemberServiceRolePolicy es una [política administrada porAWS](#) que: brinda un rol de servicio para CloudFormation StackSets (cuenta de miembro de Organization)

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de diciembre de 2019 a las 23:52 UTC
- Hora de edición: 9 de diciembre de 2019 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:GetRole"
      ]
    }
  ]
}
```

```
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:iam::*:role/stacksets-exec-*"
    ]
  },
  {
    "Action" : [
      "iam:DetachRolePolicy",
      "iam:AttachRolePolicy"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:iam::*:role/stacksets-exec-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
      }
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudFrontFullAccess

CloudFrontFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a la CloudFront consola, además de la posibilidad de publicar buckets de Amazon S3 a través delAWS Management Console.

Uso de la política

Puede asociar CloudFrontFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 4 de enero de 2024 a las 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudFrontReadOnlyAccess

CloudFrontReadOnlyAccesses una [política AWS administrada](#) que: proporciona acceso a la información de configuración CloudFront de la distribución y enumera las distribuciones a través deAWS Management Console.

Uso de la política

Puede asociar `CloudFrontReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora editada: 4 de enero de 2024 a las 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudHSMServiceRolePolicy

CloudHSMServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a los recursos AWS utilizados o gestionados por CloudHSM

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de noviembre de 2017 a las 19:12 UTC
- Hora de edición: 6 de noviembre de 2017 a las 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudSearchFullAccess

CloudSearchFullAccess es una [política administrada por AWS](#) que: proporciona acceso total al servicio de configuración de Amazon CloudSearch.

Uso de la política

Puede asociar CloudSearchFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudSearchReadOnlyAccess

CloudSearchReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura al servicio de configuración de Amazon CloudSearch.

Uso de la política

Puede asociar CloudSearchReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudTrailServiceRolePolicy

CloudTrailServiceRolePolicy es una [política AWS gestionada](#) que: Política de permisos para CloudTrail ServiceLinkedRole

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de octubre de 2018 a las 21:21 UTC
- Hora editada: 27 de noviembre de 2023 a las 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTableAccess",
      "Effect" : "Allow",
      "Action" : "glue:DeleteTable",
```

```
"Resource" : [
  "arn:*:glue:*:*:catalog",
  "arn:*:glue:*:*:database/aws:cloudtrail",
  "arn:*:glue:*:*:table/aws:cloudtrail/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "DeregisterResourceAccess",
  "Effect" : "Allow",
  "Action" : "lakeformation:DeregisterResource",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatch-CrossAccountAccess

CloudWatch-CrossAccountAccess es una [política administrada por AWS](#) que: permite a CloudWatch asumir los roles CloudWatch-CrossAccountSharing en cuentas remotas en nombre de la cuenta actual para mostrar datos entre cuentas y regiones

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de julio de 2019 a las 09:59 UTC
- Hora de edición: 23 de julio de 2019 a las 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchActionsEC2Access

CloudWatchActionsEC2Access es una [política administrada por AWS](#) que: concede acceso de solo lectura a alarmas y métricas de CloudWatch, y a los metadatos de EC2. Proporciona acceso a las instancias de EC2 para detener, terminar y reiniciar.

Uso de la política

Puede asociar CloudWatchActionsEC2Access a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de julio de 2015 a las 00:00 UTC
- Hora de edición: 7 de julio de 2015 a las 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ]
    }
  ],
}
```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchAgentAdminPolicy

CloudWatchAgentAdminPolicy es una [política AWS gestionada](#) que: se requieren permisos completos para su uso AmazonCloudWatchAgent.

Uso de la política

Puede asociar CloudWatchAgentAdminPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de marzo de 2018 a las 00:52 UTC
- Hora editada: 5 de febrero de 2024 a las 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchAgentServerPolicy

CloudWatchAgentServerPolicy es una [política AWS administrada](#) que: Se requieren permisos para su uso AmazonCloudWatchAgent en los servidores

Uso de la política

Puede asociar CloudWatchAgentServerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de marzo de 2018 a las 01:06 UTC
- Hora editada: 6 de febrero de 2024 a las 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "ec2:DescribeVolumes",
    "ec2:DescribeTags",
    "logs:PutLogEvents",
    "logs:PutRetentionPolicy",
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups",
    "logs:CreateLogStream",
    "logs:CreateLogGroup",
    "xray:PutTraceSegments",
    "xray:PutTelemetryRecords",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetSamplingStatisticSummaries"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CWASSMServerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchApplicationInsightsFullAccess

CloudWatchApplicationInsightsFullAccess es una [política administrada por AWS](#) que brinda acceso total a CloudWatch Application Insights y a las dependencias requeridas.

Uso de la política

Puede asociar `CloudWatchApplicationInsightsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de noviembre de 2020 a las 18:44 UTC
- Hora de edición: 25 de enero de 2022 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
```

```

    "autoscaling:DescribeAutoScalingGroups",
    "lambda:ListFunctions",
    "dynamodb:ListTables",
    "s3:ListAllMyBuckets",
    "sns:ListTopics",
    "states:ListStateMachines",
    "apigateway:GET",
    "ecs:ListClusters",
    "ecs:DescribeTaskDefinition",
    "ecs:ListServices",
    "ecs:ListTasks",
    "eks:ListClusters",
    "eks:ListNodegroups",
    "fsx:DescribeFileSystems",
    "logs:DescribeLogGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "application-insights.amazonaws.com"
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchApplicationInsightsReadOnlyAccess

CloudWatchApplicationInsightsReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a CloudWatch Application Insights.

Uso de la política

Puede asociar CloudWatchApplicationInsightsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de noviembre de 2020 a las 18:48 UTC
- Hora de edición: 24 de noviembre de 2020 a las 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

CloudwatchApplicationInsightsServiceLinkedRolePolicy es una [política administrada por AWS](#) que: es una Política de roles vinculados a un servicio para Cloudwatch Application Insights Service

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de diciembre de 2018 a las 16:22 UTC
- Hora de edición: 11 de mayo de 2023 a las 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v24 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchApplicationSignalsServiceRolePolicy

CloudWatchApplicationSignalsServiceRolePolicy es una [política AWS administrada](#) que: La política otorga permiso a CloudWatch Application Signals para recopilar datos de monitoreo y etiquetado de otros AWS servicios relevantes.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de noviembre de 2023 a las 18:09 UTC
- Hora editada: 7 de marzo de 2024 a las 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
```

```
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "CWLogsPermission",
  "Effect" : "Allow",
  "Action" : [
    "logs:StartQuery",
    "logs:GetQueryResults"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${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}"
    }
  }
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

CloudWatchAutomaticDashboardsAccess

CloudWatchAutomaticDashboardsAccess es una [política administrada por AWS](#) que: brinda acceso a las API ajenas a CloudWatch que se utilizan para mostrar los paneles automáticos de CloudWatch, incluido el contenido de los objetos, como las funciones de Lambda

Uso de la política

Puede asociar CloudWatchAutomaticDashboardsAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de julio de 2019 a las 10:01 UTC
- Hora de edición: 20 de abril de 2021 a las 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
```



```
    "sns:ListTopics",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "sqs:ListQueues",
    "synthetics:DescribeCanariesLastRun",
    "tag:GetResources"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "apigateway:GET"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:apigateway:*::/restapis*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchCrossAccountSharingConfiguration

CloudWatchCrossAccountSharingConfiguration es una [política administrada por AWS](#) que: brinda capacidades para gestionar los enlaces de Observability Access Manager y establecer el uso compartido de los recursos de CloudWatch

Uso de la política

Puede asociar `CloudWatchCrossAccountSharingConfiguration` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2022 a las 14:01 UTC
- Hora de edición: 27 de noviembre de 2022 a las 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam>DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
    },
  ],
}
```

```
    "Resource" : "arn:aws:oam:*:*:link/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "oam:CreateLink",
      "oam:UpdateLink"
    ],
    "Resource" : [
      "arn:aws:oam:*:*:link/*",
      "arn:aws:oam:*:*:sink/*"
    ]
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchEventsBuiltInTargetExecutionAccess

CloudWatchEventsBuiltInTargetExecutionAccess es una [política administrada por AWS](#) que: permite que los objetivos integrados en los Eventos de Amazon CloudWatch realicen acciones de EC2 en su nombre.

Uso de la política

Puede asociar CloudWatchEventsBuiltInTargetExecutionAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 14 de enero de 2016 a las 18:35 UTC
- Hora de edición: 14 de enero de 2016 a las 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchEventsFullAccess

CloudWatchEventsFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a los Eventos de Amazon CloudWatch.

Uso de la política

Puede asociar CloudWatchEventsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de enero de 2016 a las 18:37 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
```

```

    "pipes:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
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"
      }
    }
  }
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchEventsInvocationAccess

CloudWatchEventsInvocationAccess es una [política administrada por AWS](#) que: permite que los Eventos de Amazon CloudWatch retransmitan los eventos a las transmisiones de Kinesis Streams de AWS de su cuenta.

Uso de la política

Puede asociar CloudWatchEventsInvocationAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de enero de 2016 a las 18:36 UTC
- Hora de edición: 14 de enero de 2016 a las 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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



```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchEventsReadOnlyAccess

CloudWatchEventsReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a los Eventos de Amazon CloudWatch.

Uso de la política

Puede asociar CloudWatchEventsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 14 de enero de 2016 a las 18:27 UTC
- Hora de edición: 1 de diciembre de 2022 a las 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
```

```
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchEventsServiceRolePolicy

CloudWatchEventsServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS CloudWatch ejecute acciones en su nombre configuradas mediante alarmas y eventos.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2017 a las 00:42 UTC
- Hora de edición: 17 de noviembre de 2017 a las 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchFullAccess

CloudWatchFullAccess es una [política administrada por AWS](#) que: brinda acceso total a CloudWatch.

Uso de la política

Puede asociar CloudWatchFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
```

```
        "iam:GetRole",
        "oam:ListSinks"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "events.amazonaws.com"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "oam:ListAttachedLinks"
    ],
    "Resource" : "arn:aws:oam::*:sink/*"
}
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchFullAccessV2

CloudWatchFullAccessV2 es una [política AWS gestionada](#) que: Proporciona acceso total a CloudWatch.

Uso de la política

Puede asociar `CloudWatchFullAccessV2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de agosto de 2023 a las 11:32 UTC
- Hora editada: 5 de diciembre de 2023 a las 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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/*"
}
]
}

```


Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchInternetMonitorServiceRolePolicy

CloudWatchInternetMonitorServiceRolePolicy es una [política administrada por AWS](#) que: permite que Internet Monitor acceda a los recursos de EC2, Workspaces y CloudFront y a otros servicios necesarios en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de noviembre de 2022 a las 17:46 UTC
- Hora de edición: 20 de julio de 2023 a las 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/InternetMonitor"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchLambdaInsightsExecutionRolePolicy

CloudWatchLambdaInsightsExecutionRolePolicy es una [política administrada por AWS](#) que: se requiere para la Extensión Lambda Insights

Uso de la política

Puede asociar CloudWatchLambdaInsightsExecutionRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de octubre de 2020 a las 19:27 UTC
- Hora de edición: 7 de octubre de 2020 a las 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : "logs:CreateLogGroup",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchLogsCrossAccountSharingConfiguration

CloudWatchLogsCrossAccountSharingConfiguration es una [política administrada por AWS](#) que: proporciona funciones para gestionar los enlaces de Observability Access Manager y establecer el uso compartido de los recursos de los Registros de CloudWatch

Uso de la política

Puede asociar CloudWatchLogsCrossAccountSharingConfiguration a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 27 de noviembre de 2022 a las 13:55 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam>DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
    },
  ]
}
```

```
    "Resource" : [  
      "arn:aws:oam:*:*:link/*",  
      "arn:aws:oam:*:*:sink/*"  
    ]  
  }  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchLogsFullAccess

CloudWatchLogsFullAccesses una [política AWS gestionada](#) que: proporciona acceso total a CloudWatch los registros

Uso de la política

Puede asociar CloudWatchLogsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 26 de noviembre de 2023 a las 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchLogsReadOnlyAccess

CloudWatchLogsReadOnlyAccesses una [política AWS administrada](#) que: Proporciona acceso de solo lectura a CloudWatch los registros

Uso de la política

Puede asociar CloudWatchLogsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 26 de noviembre de 2023 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```


Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchNetworkMonitorServiceRolePolicy

CloudWatchNetworkMonitorServiceRolePolicy es una [política AWS gestionada](#) que: permite a CloudWatch Network Monitor acceder a los recursos de EC2 y VPC y gestionarlos, publicar datos y acceder CloudWatch a otros servicios necesarios en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de diciembre de 2023 a las 18:53 UTC
- Hora editada: 21 de diciembre de 2023 a las 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
```

```
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchReadOnlyAccess

CloudWatchReadOnlyAccesses una [política AWS gestionada](#) que: Proporciona acceso de solo lectura a CloudWatch.

Uso de la política

Puede asociar CloudWatchReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 5 de diciembre de 2023 a las 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchSyntheticsFullAccess

CloudWatchSyntheticsFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a CloudWatch Synthetics.

Uso de la política

Puede asociar CloudWatchSyntheticsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de noviembre de 2019 a las 17:39 UTC
- Hora de edición: 6 de mayo de 2022 a las 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces",
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
"Action" : [
  "s3:GetBucketLocation"
],
"Resource" : "arn:aws:s3:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::cw-syn-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "synthetics.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
```

```
    "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch>DeleteAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "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"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CloudWatchSyntheticsReadOnlyAccess

CloudWatchSyntheticsReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura a CloudWatch Synthetics.

Uso de la política

Puede asociar CloudWatchSyntheticsReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de noviembre de 2019 a las 17:45 UTC
- Hora de edición: 6 de marzo de 2020 a las 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ComprehendDataAccessRolePolicy

ComprehendDataAccessRolePolicy es una [política administrada por AWS](#) que: es una política para el rol de servicio de AWS Comprehend que concede acceso a los recursos de S3 para acceder a los datos

Uso de la política

Puede asociar ComprehendDataAccessRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de marzo de 2019 a las 22:28 UTC
- Hora de edición: 6 de marzo de 2019 a las 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*Comprehend*",
      "arn:aws:s3::*comprehend*"
    ]
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ComprehendFullAccess

ComprehendFullAccess es una [política administrada por AWS](#) que: otorga acceso total a Amazon Comprehend.

Uso de la política

Puede asociar ComprehendFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 29 de noviembre de 2017 a las 18:08 UTC
- Hora de edición: 5 de diciembre de 2017 a las 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ComprehendMedicalFullAccess

ComprehendMedicalFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Comprehend Medical

Uso de la política

Puede asociar ComprehendMedicalFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2018 a las 17:55 UTC
- Hora de edición: 27 de noviembre de 2018 a las 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ComprehendReadOnly

ComprehendReadOnly es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Amazon Comprehend.

Uso de la política

Puede asociar ComprehendReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2017 a las 18:10 UTC
- Hora de edición: 26 de abril de 2022 a las 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectDominantLanguage",
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:DetectEntities",
        "comprehend:BatchDetectEntities",
        "comprehend:DetectKeyPhrases",
        "comprehend:BatchDetectKeyPhrases",
        "comprehend:DetectPiiEntities",
        "comprehend:ContainsPiiEntities",
        "comprehend:DetectSentiment",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectSyntax",
        "comprehend:BatchDetectSyntax",
        "comprehend:ClassifyDocument",
        "comprehend:DescribeTopicsDetectionJob",
        "comprehend:ListTopicsDetectionJobs",
        "comprehend:DescribeDominantLanguageDetectionJob",
        "comprehend:ListDominantLanguageDetectionJobs",
        "comprehend:DescribeEntitiesDetectionJob",
        "comprehend:ListEntitiesDetectionJobs",
        "comprehend:DescribeKeyPhrasesDetectionJob",
        "comprehend:ListKeyPhrasesDetectionJobs",
        "comprehend:DescribePiiEntitiesDetectionJob",
        "comprehend:ListPiiEntitiesDetectionJobs",
        "comprehend:DescribeSentimentDetectionJob",
        "comprehend:DescribeTargetedSentimentDetectionJob",
        "comprehend:ListSentimentDetectionJobs",
        "comprehend:ListTargetedSentimentDetectionJobs",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:ListDocumentClassifiers",
        "comprehend:DescribeDocumentClassificationJob",
        "comprehend:ListDocumentClassificationJobs",
        "comprehend:DescribeEntityRecognizer",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListTagsForResource",
        "comprehend:DescribeEndpoint",
```

```
        "comprehend:ListEndpoints",
        "comprehend:ListDocumentClassifierSummaries",
        "comprehend:ListEntityRecognizerSummaries",
        "comprehend:DescribeResourcePolicy"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ComputeOptimizerReadOnlyAccess

ComputeOptimizerReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura a ComputeOptimizer.

Uso de la política

Puede asociar ComputeOptimizerReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 7 de marzo de 2020 a las 00:11 UTC
- Hora de edición: 28 de agosto de 2023 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ComputeOptimizerServiceRolePolicy

ComputeOptimizerServiceRolePolicy es una [política administrada por AWS](#) que: permite que ComputeOptimizer llame a los servicios de AWS y recopile información de la carga de trabajo en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2019 a las 08:45 UTC
- Hora de edición: 13 de junio de 2022 a las 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
```

```
    "autoscaling:DescribeAutoScalingGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2Access",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes"
  ],
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ConfigConformsServiceRolePolicy

ConfigConformsServiceRolePolicy es una [política administrada por AWS](#) que: es necesaria para que AWSConfig cree paquetes de conformidad

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de julio de 2019 a las 21:38 UTC
- Hora de edición: 12 de enero de 2023 a las 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config>DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeRemediationConfigurations",
        "config>DeleteRemediationConfiguration",
        "config:PutRemediationConfigurations"
      ],
      "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-remediation-configuration/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "remediation.config.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:GetDocument"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [

```



```

    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:GetObject",
    "s3:GetBucketAcl"
  ],
  "Resource" : "arn:aws:s3:::awsconfigconforms*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:GetStackPolicy",
    "cloudformation:SetStackPolicy",
    "cloudformation:UpdateStack",
    "cloudformation:UpdateTerminationProtection",
    "cloudformation:ValidateTemplate",
    "cloudformation:ListStackResources"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/Config"
    }
  }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CostOptimizationHubAdminAccess

CostOptimizationHubAdminAccesses una [política AWS gestionada](#) que: Esta política gestionada proporciona acceso de administrador a Cost Optimization Hub.

Uso de la política

Puede asociar CostOptimizationHubAdminAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de diciembre de 2023 a las 00:03 UTC
- Hora editada: 19 de diciembre de 2023 a las 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
```

```

    "cost-optimization-hub:UpdatePreferences",
    "cost-optimization-hub:GetRecommendation",
    "cost-optimization-hub:ListRecommendations",
    "cost-optimization-hub:ListRecommendationSummaries"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "organizations:ServicePrincipal" : [
        "cost-optimization-hub.bcm.amazonaws.com"
      ]
    }
  }
}
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CostOptimizationHubReadOnlyAccess

CostOptimizationHubReadOnlyAccesses una [política AWS gestionada](#) que: Esta política gestionada proporciona acceso de solo lectura a Cost Optimization Hub.

Uso de la política

Puede asociar CostOptimizationHubReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de diciembre de 2023 a las 18:04 UTC
- Hora editada: 13 de diciembre de 2023 a las 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Sid" : "CostOptimizationHubReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "cost-optimization-hub:ListEnrollmentStatuses",
      "cost-optimization-hub:GetPreferences",
      "cost-optimization-hub:GetRecommendation",
      "cost-optimization-hub:ListRecommendations",
      "cost-optimization-hub:ListRecommendationSummaries"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CostOptimizationHubServiceRolePolicy

CostOptimizationHubServiceRolePolicy es una [política AWS gestionada](#) que: permite a Cost Optimization Hub recuperar información de la organización y recopilar datos y metadatos relacionados con la optimización.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 26 de noviembre de 2023 a las 08:03 UTC
- Hora editada: 26 de noviembre de 2023 a las 08:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

CustomerProfilesServiceLinkedRolePolicy

CustomerProfilesServiceLinkedRolePolicy es una [política administrada por AWS](#) que: permite que los perfiles de clientes de Amazon Connect accedan a los servicios de AWS y recursos en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de marzo de 2023 a las 22:56 UTC
- Hora de edición: 7 de marzo de 2023 a las 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/CustomerProfiles"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/
AWSServiceRoleForProfile_*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

DatabaseAdministrator

DatabaseAdministrator es una [política administrada por AWS](#) que: concede permisos de acceso total a los servicios de AWS y las acciones necesarios para instalar y configurar los servicios de bases de datos de AWS.

Uso de la política

Puede asociar DatabaseAdministrator a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:25 UTC
- Hora de edición: 8 de enero de 2019 a las 00:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline>DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
```

```
    "datapipeline:ListPipelines",
    "datapipeline:PutPipelineDefinition",
    "datapipeline:QueryObjects",
    "dynamodb:*",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "elasticache:*",
    "iam:ListRoles",
    "iam:GetRole",
    "kms:ListKeys",
    "lambda:CreateEventSourceMapping",
    "lambda:CreateFunction",
    "lambda>DeleteEventSourceMapping",
    "lambda>DeleteFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:ListEventSourceMappings",
    "lambda:ListFunctions",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:FilterLogEvents",
    "logs:GetLogEvents",
    "logs:Create*",
    "logs:PutLogEvents",
    "logs:PutMetricFilter",
    "rds:*",
    "redshift:*",
    "s3:CreateBucket",
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:Get*",
    "sns:List*",
    "sns:SetTopicAttributes",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
```

```

    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject*",
      "s3:Get*",
      "s3:List*",
      "s3:PutAccelerateConfiguration",
      "s3:PutBucketTagging",
      "s3:PutBucketVersioning",
      "s3:PutBucketWebsite",
      "s3:PutLifecycleConfiguration",
      "s3:PutReplicationConfiguration",
      "s3:PutObject*",
      "s3:Replicate*",
      "s3:RestoreObject"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/rds-monitoring-role",
      "arn:aws:iam::*:role/rdbms-lambda-access",
      "arn:aws:iam::*:role/lambda_exec_role",
      "arn:aws:iam::*:role/lambda-dynamodb-*",
      "arn:aws:iam::*:role/lambda-vpc-execution-role",
      "arn:aws:iam::*:role/DataPipelineDefaultRole",
      "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
    ]
  }
]
}

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

DataScientist

DataScientist es una [política administrada por AWS](#) que: concede permisos a los servicios de análisis de datos de AWS.

Uso de la política

Puede asociar DataScientist a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:28 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:CreateStack",
```

```
"cloudformation:DescribeStackEvents",
"datapipeline:Describe*",
"datapipeline:ListPipelines",
"datapipeline:GetPipelineDefinition",
"datapipeline:QueryObjects",
"dynamodb:*",
"ec2:CancelSpotInstanceRequests",
"ec2:CancelSpotFleetRequests",
"ec2:CreateTags",
"ec2>DeleteTags",
"ec2:Describe*",
"ec2:ModifyImageAttribute",
"ec2:ModifyInstanceAttribute",
"ec2:ModifySpotFleetRequest",
"ec2:RequestSpotInstances",
"ec2:RequestSpotFleet",
"elasticfilesystem:*",
"elasticmapreduce:*",
"es:*",
"firehose:*",
"fsx:DescribeFileSystems",
"iam:GetInstanceProfile",
"iam:GetRole",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:ListRoles",
"kinesis:*",
"kms:List*",
"lambda:Create*",
"lambda>Delete*",
"lambda:Get*",
"lambda:InvokeFunction",
"lambda:PublishVersion",
"lambda:Update*",
"lambda:List*",
"machinelearning:*",
"sdb:*",
"rds:*",
"sns:ListSubscriptions",
"sns:ListTopics",
"logs:DescribeLogStreams",
"logs:GetLogEvents",
"redshift:*",
"s3:CreateBucket",
```

```
    "sns:CreateTopic",
    "sns:Get*",
    "sns:List*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:Abort*",
    "s3:DeleteObject",
    "s3:Get*",
    "s3:List*",
    "s3:PutAccelerateConfiguration",
    "s3:PutBucketCors",
    "s3:PutBucketLogging",
    "s3:PutBucketNotification",
    "s3:PutBucketTagging",
    "s3:PutObject",
    "s3:Replicate*",
    "s3:RestoreObject"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/DataPipelineDefaultRole",
```

```

    "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
    "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
    "arn:aws:iam::*:role/EMR_DefaultRole",
    "arn:aws:iam::*:role/kinesis-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "sagemaker.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:*"
  ],
  "NotResource" : [
    "arn:aws:sagemaker::*:domain/*",
    "arn:aws:sagemaker::*:user-profile/*",
    "arn:aws:sagemaker::*:app/*",
    "arn:aws:sagemaker::*:flow-definition/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreatePresignedDomainUrl",
    "sagemaker:DescribeDomain",
    "sagemaker:ListDomains",
    "sagemaker:DescribeUserProfile",
    "sagemaker:ListUserProfiles",
    "sagemaker:*App",
    "sagemaker:ListApps"
  ],
  "Resource" : "*"
},
{

```

```
"Effect" : "Allow",
"Action" : [
  "sagemaker:*FlowDefinition",
  "sagemaker:*FlowDefinitions"
],
"Resource" : "*",
"Condition" : {
  "StringEqualsIfExists" : {
    "sagemaker:WorkteamType" : [
      "private-crowd",
      "vendor-crowd"
    ]
  }
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

DAXServiceRolePolicy

DAXServiceRolePolicy es una [política administrada por AWS](#) que: permite que DAX cree y administre la interfaz de red, el grupo de seguridad, la subred y la VPC en nombre del cliente

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de marzo de 2018 a las 17:51 UTC
- Hora de edición: 5 de marzo de 2018 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

DynamoDBCloudWatchContributorInsightsServiceRolePolicy es una [política administrada por AWS](#) que: requiere permisos para brindar soporte a la Información de colaboradores de Amazon CloudWatch para Amazon DynamoDB.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2019 a las 21:13 UTC
- Hora de edición: 15 de noviembre de 2019 a las 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Action" : [
      "cloudwatch:DeleteInsightRules",
      "cloudwatch:PutInsightRule"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
  },
  {
    "Action" : [
      "cloudwatch:DescribeInsightRules"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

DynamoDBKinesisReplicationServiceRolePolicy

DynamoDBKinesisReplicationServiceRolePolicy es una [política administrada por AWS](#) que: concede acceso a DynamoDB de AWS a KinesisDataStreams

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de noviembre de 2020 a las 00:43 UTC
- Hora de edición: 12 de noviembre de 2020 a las 00:43 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

DynamoDBReplicationServiceRolePolicy

DynamoDBReplicationServiceRolePolicy es una [política administrada por AWS](#) que: requiere permisos por DynamoDB para la replicación de datos entre regiones

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de noviembre de 2017 a las 23:55 UTC
- Hora editada: 8 de enero de 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "dynamodb:GetItem",
    "dynamodb:PutItem",
    "dynamodb:UpdateItem",
    "dynamodb>DeleteItem",
    "dynamodb:DescribeTable",
    "dynamodb:UpdateTable",
    "dynamodb:Scan",
    "dynamodb:DescribeStream",
    "dynamodb:GetRecords",
    "dynamodb:GetShardIterator",
    "dynamodb:DescribeTimeToLive",
    "dynamodb:UpdateTimeToLive",
    "dynamodb:DescribeLimits",
    "dynamodb:GetResourcePolicy",
    "application-autoscaling:RegisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:DescribeScalingPolicies",
    "account:ListRegions"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DynamoDBReplicationServiceRolePolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "dynamodb.application-autoscaling.amazonaws.com"
      ]
    }
  }
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

EC2FastLaunchServiceRolePolicy

EC2FastLaunchServiceRolePolicy es una [política administrada por AWS](#) que: permite que ec2fastlaunch prepare y gestione las capturas se aprovisionaron previamente en la cuenta del cliente y publique las métricas relacionadas.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de enero de 2022 a las 13:08 UTC
- Hora de edición: 10 de enero de 2022 a las 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "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:DescribeInstanceState",
  "ec2:DescribeInstances",
  "ec2:DescribeInstanceTypeOfferings",
  "ec2:DescribeLaunchTemplateVersions",
  "ec2:DescribeLaunchTemplates"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/EC2"
    }
  }
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

EC2FleetTimeShiftableServiceRolePolicy

EC2FleetTimeShiftableServiceRolePolicy es una [política administrada por AWS](#) que otorga permisos a EC2 Fleet para lanzar instancias en el futuro.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de diciembre de 2019 a las 19:47 UTC
- Hora de edición: 23 de diciembre de 2019 a las 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
  ],
}
```

```
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:spot-instances-request/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

Ec2ImageBuilderCrossAccountDistributionAccess

Ec2ImageBuilderCrossAccountDistributionAccess es una [política administrada por AWS](#) que: otorga los permisos que necesita EC2 Image Builder para realizar una distribución entre cuentas.

Uso de la política

Puede asociar Ec2ImageBuilderCrossAccountDistributionAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de septiembre de 2020 a las 19:22 UTC
- Hora de edición: 30 de septiembre de 2020 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*::image/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:CopyImage",
      "ec2:ModifyImageAttribute"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

EC2ImageBuilderLifecycleExecutionPolicy

EC2ImageBuilderLifecycleExecutionPolicy es una [política AWS gestionada](#) que: la ImageBuilderLifecycleExecutionPolicy política de EC2 concede permisos para que Image Builder lleve a cabo acciones como desaprobar o eliminar los recursos de imagen de Image Builder y sus recursos subyacentes (AMI, instantáneas) a fin de admitir reglas automatizadas para las tareas de administración del ciclo de vida de las imágenes.

Uso de la política

Puede asociar EC2ImageBuilderLifecycleExecutionPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 16 de noviembre de 2023 a las 23:23 UTC
- Hora editada: 16 de noviembre de 2023 a las 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
  ],
}
```



```

    "Sid" : "EC2DeleteSnapshotPermission",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteSnapshot",
    "Resource" : "arn:aws:ec2:*::snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      }
    }
  },
  {
    "Sid" : "EC2TagsPermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteTags",
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*::snapshot/*",
      "arn:aws:ec2:*::image/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
        "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "DeprecatedBy"
      }
    }
  },
  {
    "Sid" : "ECRIImagePermission",
    "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" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

EC2InstanceConnect

EC2InstanceConnect es una [política administrada por AWS](#) que: permite que los clientes llamen a EC2 Instance Connect para publicar claves efímeras en sus instancias EC2 y se conecten mediante ssh o CLI de EC2 Instance Connect.

Uso de la política

Puede asociar EC2InstanceConnect a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de junio de 2019 a las 18:53 UTC
- Hora de edición: 27 de junio de 2019 a las 18:53 UTC

- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

Ec2InstanceConnectEndpoint

Ec2InstanceConnectEndpoint es una [política administrada por AWS](#) que: otorga la Política de puntos de conexión de Instance Connect de EC2 para gestionar los puntos de conexión de EC2 Instance Connect que creó el cliente

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de enero de 2023 a las 20:19 UTC
- Hora de edición: 24 de enero de 2023 a las 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:subnet/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "InstanceConnectEndpointId"
      ]
    },
    "Null" : {
      "aws:RequestTag/InstanceConnectEndpointId" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/InstanceConnectEndpointId" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
```

```
    "ec2:CreateAction" : "CreateNetworkInterface"
  },
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "InstanceConnectEndpointId"
    ]
  },
  "Null" : {
    "aws:RequestTag/InstanceConnectEndpointId" : "false"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteNetworkInterface"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/InstanceConnectEndpointId" : [
        "eice-*"
      ]
    }
  }
}
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

EC2InstanceProfileForImageBuilder

EC2InstanceProfileForImageBuilder es una [política administrada por AWS](#) que: brinda un perfil de instancia EC2 para el servicio Image Builder.

Uso de la política

Puede asociar `EC2InstanceProfileForImageBuilder` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de diciembre de 2019 a las 19:08 UTC
- Hora de edición: 27 de agosto de 2020 a las 16:40 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

EC2InstanceProfileForImageBuilderECRContainerBuilds es una [política administrada por AWS](#) que: brinda un perfil de instancia EC2 para crear imágenes de contenedores con EC2 Image Builder. Esta política otorga al usuario amplios permisos para cargar imágenes de ECR.

Uso de la política

Puede asociar `EC2InstanceProfileForImageBuilderECRContainerBuilds` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de diciembre de 2020 a las 19:48 UTC
- Hora de edición: 11 de diciembre de 2020 a las 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ]
    }
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:Decrypt"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
        "aws:CalledVia" : [
          "imagebuilder.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::ec2imagebuilder*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ECRReplicationServiceRolePolicy

ECRReplicationServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y los recursos utilizados o administrados por ECR Replication

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de diciembre de 2020 a las 22:11 UTC
- Hora de edición: 4 de diciembre de 2020 a las 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElastiCacheServiceRolePolicy

ElastiCacheServiceRolePolicy es una [política AWS administrada](#) que: Esta política permite ElastiCache administrar AWS los recursos en su nombre según sea necesario para administrar la memoria caché

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de diciembre de 2017 a las 17:50 UTC
- Hora editada: 28 de noviembre de 2023 a las 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
```

```

    "StringLike" : {
      "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
    }
  },
  {
    "Sid" : "TagVPCEndpointsOnCreation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint",
        "aws:RequestTag/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/*"
  }
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElasticLoadBalancingFullAccess

ElasticLoadBalancingFullAccess es una [política administrada por AWS](#) que: brinda acceso total a Amazon ElasticLoadBalancing y acceso limitado a otros servicios necesarios para proporcionar las características de ElasticLoadBalancing.

Uso de la política

Puede asociar ElasticLoadBalancingFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de septiembre de 2018 a las 20:42 UTC
- Hora de edición: 29 de noviembre de 2022 a las 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Action" : "elasticloadbalancing:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAddresses",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcClassicLink",
      "ec2:DescribeInstances",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeClassicLinkInstances",
      "ec2:DescribeRouteTables",
      "ec2:DescribeCoipPools",
      "ec2:GetCoipPoolUsage",
      "ec2: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" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElasticLoadBalancingReadOnly

ElasticLoadBalancingReadOnly es una [política AWS gestionada](#) que: proporciona acceso de solo lectura a Amazon ElasticLoadBalancing y a los servicios dependientes

Uso de la política

Puede asociar ElasticLoadBalancingReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 20 de septiembre de 2018 a las 20:17 UTC
- Hora editada: 26 de noviembre de 2023 a las 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement3",
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:GetManagedResource",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Sid" : "Statement4",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElementalActivationsDownloadSoftwareAccess

ElementalActivationsDownloadSoftwareAccess es una [política administrada por AWS](#) que: permite ver los activos comprados y descargar el software relacionado y los archivos de inicio

Uso de la política

Puede asociar ElementalActivationsDownloadSoftwareAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 8 de septiembre de 2020 a las 17:26 UTC
- Hora de edición: 8 de septiembre de 2020 a las 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElementalActivationsFullAccess

ElementalActivationsFullAccess es una [política administrada por AWS](#): que ofrece acceso total para ver los activos comprados por Elemental Appliances y Software y tomar medidas al respecto

Uso de la política

Puede asociar ElementalActivationsFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 4 de junio de 2020 a las 21:00 UTC
- Hora de edición: 4 de junio de 2020 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElementalActivationsGenerateLicenses

ElementalActivationsGenerateLicenses es una [política administrada por AWS](#) que: permite ver los activos comprados y generar licencias de software para las activaciones pendientes

Uso de la política

Puede asociar ElementalActivationsGenerateLicenses a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de agosto de 2020 a las 18:28 UTC
- Hora de edición: 28 de agosto de 2020 a las 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElementalActivationsReadOnlyAccess

`ElementalActivationsReadOnlyAccess` es una [política administrada por AWS](#) que: permite el acceso de solo lectura a la lista detallada de los activos comprados asociados al usuario de Cuenta de AWS

Uso de la política

Puede asociar `ElementalActivationsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 28 de agosto de 2020 a las 16:51 UTC
- Hora de edición: 28 de agosto de 2020 a las 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElementalAppliancesSoftwareFullAccess

ElementalAppliancesSoftwareFullAccess es una [política administrada por AWS](#) que: otorga acceso total para ver las cotizaciones y los pedidos de Elemental Appliances and Software y tomar medidas al respecto

Uso de la política

Puede asociar ElementalAppliancesSoftwareFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS

- Hora de creación: 31 de julio de 2019 a las 16:28 UTC
- Hora de edición: 5 de febrero de 2021 a las 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElementalAppliancesSoftwareReadOnlyAccess

ElementalAppliancesSoftwareReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura para ver las cotizaciones y los pedidos de Elemental Appliances y Software

Uso de la política

Puede asociar ElementalAppliancesSoftwareReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 1 de abril de 2020 a las 22:31 UTC
- Hora de edición: 1 de abril de 2020 a las 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ElementalSupportCenterFullAccess

`ElementalSupportCenterFullAccess` es una [política administrada por AWS](#) que ofrece acceso total para ver los casos de soporte de Elemental Appliance and Software y el contenido de soporte de productos y tomar medidas al respecto

Uso de la política

Puede asociar `ElementalSupportCenterFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de noviembre de 2020 a las 18:08 UTC
- Hora de edición: 5 de febrero de 2021 a las 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

EMRDescribeClusterPolicyForEMRWAL

EMRDescribeClusterPolicyForEMRWAL es una [política administrada por AWS](#) que: concede permisos de solo lectura que permiten al servicio WAL de Amazon EMR encontrar y devolver el estado de un clúster

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de junio de 2023 a las 23:30 UTC
- Hora de edición: 15 de junio de 2023 a las 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

FMSServiceRolePolicy

FMSServiceRolePolicy es una [Política de acceso administrada por AWS](#) que: permite que el rol vinculado a un servicio de FM realice acciones relacionadas con FM en los recursos administrados por FM dentro de la cuenta de AWS Organization de un cliente.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 28 de marzo de 2018 a las 23:01 UTC
- Hora de edición: 21 de abril de 2023 a las 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Versión de la política

Versión de la política: v28 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
```

```

    "waf-regional:UpdateWebACL",
    "waf-regional>DeleteWebACL",
    "waf-regional:GetWebACL",
    "waf-regional:GetRuleGroup",
    "waf-regional>ListSubscribedRuleGroups",
    "waf-regional>ListResourcesForWebACL",
    "waf-regional:AssociateWebACL",
    "waf-regional:DisassociateWebACL",
    "elasticloadbalancing:SetWebACL",
    "apigateway:SetWebACL",
    "elasticloadbalancing:SetSecurityGroups",
    "waf:ListTagsForResource",
    "waf-regional:ListTagsForResource"
  ],
  "Resource" : [
    "arn:aws:waf:*:*:webacl/*",
    "arn:aws:waf-regional:*:*:webacl/*",
    "arn:aws:waf:*:*:rulegroup/*",
    "arn:aws:waf-regional:*:*:rulegroup/*",
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
    "arn:aws:apigateway:*:*:/restapis/*/stages/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutLoggingConfiguration",
    "wafv2:GetLoggingConfiguration",
    "wafv2:ListLoggingConfigurations",
    "wafv2>DeleteLoggingConfiguration"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:regional/webacl/*",
    "arn:aws:wafv2:*:*:global/webacl/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "waf:CreateWebACL",
    "waf-regional:CreateWebACL",
    "waf:GetChangeToken",
    "waf-regional:GetChangeToken",
    "waf-regional:GetWebACLForResource"
  ]
}

```

```
    ],
    "Resource" : [
      "arn:aws:waf:*:*:*",
      "arn:aws:waf-regional:*:*:*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
      "elasticloadbalancing:DescribeTags"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "waf:PutPermissionPolicy",
      "waf:GetPermissionPolicy",
      "waf>DeletePermissionPolicy",
      "waf-regional:PutPermissionPolicy",
      "waf-regional:GetPermissionPolicy",
      "waf-regional>DeletePermissionPolicy"
    ],
    "Resource" : [
      "arn:aws:waf:*:*:webacl/*",
      "arn:aws:waf:*:*:rulegroup/*",
      "arn:aws:waf-regional:*:*:webacl/*",
      "arn:aws:waf-regional:*:*:rulegroup/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudfront:GetDistribution",
      "cloudfront:UpdateDistribution",
      "cloudfront:ListDistributionsByWebACLId",
      "cloudfront:ListDistributions"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
```



```

        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation"
    ],
    "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "organizations:ListAccounts",

```

```
    "organizations:DescribeOrganizationalUnit",
    "organizations:ListChildren",
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "shield:CreateProtection",
    "shield>DeleteProtection",
    "shield:DescribeProtection",
    "shield>ListProtections",
    "shield>ListAttacks",
    "shield>CreateSubscription",
    "shield:DescribeSubscription",
    "shield:GetSubscriptionState",
    "shield:DescribeDRTAccess",
    "shield:DescribeEmergencyContactSettings",
    "shield:UpdateEmergencyContactSettings",
    "elasticloadbalancing:DescribeLoadBalancers",
    "ec2:DescribeAddresses",
    "shield:EnableApplicationLayerAutomaticResponse",
    "shield:DisableApplicationLayerAutomaticResponse",
    "shield:UpdateApplicationLayerAutomaticResponse"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
    "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
  ],
}
```

```

    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeInstances"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSecurityGroup"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteTags",
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/FMManaged" : "*"
      }
    }
  }
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup",
      "ec2:DescribeSecurityGroupReferences",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeStaleSecurityGroups",
      "ec2:DescribeNetworkInterfaces",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcPeeringConnections"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "wafv2:TagResource",
      "wafv2:ListResourcesForWebACL",
      "wafv2:AssociateWebACL",
      "wafv2:ListTagsForResource",
      "wafv2:UntagResource",
      "wafv2:GetWebACL",
      "wafv2:DisassociateFirewallManager",
      "wafv2>DeleteWebACL",
      "wafv2:DisassociateWebACL"
    ],
    "Resource" : [
      "arn:aws:wafv2:*:*:global/webacl/*",
      "arn:aws:wafv2:*:*:regional/webacl/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "wafv2:UpdateWebACL",
      "wafv2:CreateWebACL",
      "wafv2>DeleteFirewallManagerRuleGroups",
      "wafv2:PutFirewallManagerRuleGroups"
    ],
    "Resource" : [
      "arn:aws:wafv2:*:*:global/webacl/*",
      "arn:aws:wafv2:*:*:regional/webacl/*",

```

```

    "arn:aws:wafv2:*:*:global/rulegroup/*",
    "arn:aws:wafv2:*:*:regional/rulegroup/*",
    "arn:aws:wafv2:*:*:global/managedruleset/*",
    "arn:aws:wafv2:*:*:regional/managedruleset/*",
    "arn:aws:wafv2:*:*:global/ipset/*",
    "arn:aws:wafv2:*:*:regional/ipset/*",
    "arn:aws:wafv2:*:*:global/regexpatternset/*",
    "arn:aws:wafv2:*:*:regional/regexpatternset/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutPermissionPolicy",
    "wafv2:GetPermissionPolicy",
    "wafv2>DeletePermissionPolicy"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:global/rulegroup/*",
    "arn:aws:wafv2:*:*:regional/rulegroup/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudfront:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "wafv2:GetWebACLForResource"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:regional/webacl/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {

```

```
    "ec2:CreateAction" : "CreateRouteTable"
  },
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "Name",
      "FMManaged"
    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
```

```

    "Effect" : "Allow",
    "Action" : "ec2:DeleteRouteTable",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/FMManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssociateRouteTable",
      "ec2:CreateSubnet",
      "ec2:CreateRouteTable",
      "ec2>DeleteSubnet",
      "ec2:DisassociateRouteTable",
      "ec2:ReplaceRouteTableAssociation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInternetGateways",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSubnets",
      "ec2:DescribeTags",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeAvailabilityZones"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:vpc-endpoint/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/FMManaged" : [
          "true"
        ]
      }
    }
  }
]

```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateVpcEndpoint",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:vpc/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/FMManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ram:TagResource"
  ],
  "Resource" : [
    "arn:aws:ram:*:*:resource-share/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceShare",
```



```

    "ram:UpdateResourceShare",
    "ram>DeleteResourceShare"
  ],
  "Resource" : "arn:aws:ram:*:*:resource-share/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ram:CreateResourceShare",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    },
    "StringEquals" : {
      "aws:RequestTag/FMManaged" : [
        "true"
      ]
    }
  }
},
{
  "Sid" : "ram",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShareAssociations",
    "ram:GetResourceShares"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [

```

```
        "network-firewall.amazonaws.com",
        "shield.amazonaws.com"
    ]
}
},
{
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "network-firewall:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "Name",
                "FMManaged"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall>ListFirewallPolicies",
        "network-firewall>ListFirewalls",
        "network-firewall>ListRuleGroups",
```

```

    "network-firewall:PutResourcePolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall>DeleteResourcePolicy",
    "network-firewall:DescribeLoggingConfiguration",
    "network-firewall:UpdateLoggingConfiguration"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "network-firewall>DeleteFirewallPolicy",
    "network-firewall>DeleteFirewall"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:ListLogDeliveries",
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs>DeleteLogDelivery"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53resolver:ListFirewallRuleGroupAssociations",
    "route53resolver:ListTagsForResource",
    "route53resolver:ListFirewallRuleGroups",
    "route53resolver:GetFirewallRuleGroupAssociation",
    "route53resolver:GetFirewallRuleGroup",
    "route53resolver:GetFirewallRuleGroupPolicy",
    "route53resolver:PutFirewallRuleGroupPolicy"
  ],
  "Resource" : "*"
}

```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

FSxDeleteServiceLinkedRoleAccess

FSxDeleteServiceLinkedRoleAccess es una [política administrada por AWS](#) que: permite a Amazon FSx eliminar sus roles vinculados a un servicio para el acceso a Amazon S3

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 28 de noviembre de 2018 a las 10:40 UTC
- Hora de edición: 28 de noviembre de 2018 a las 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

GameLiftGameServerGroupPolicy

GameLiftGameServerGroupPolicy es una [política administrada por AWS](#) que: permite que Gamelift GameServerGroups gestione los recursos de los clientes

Uso de la política

Puede asociar GameLiftGameServerGroupPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 3 de abril de 2020 a las 23:12 UTC
- Hora de edición: 13 de mayo de 2020 a las 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
```

```

    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/GameLift" : "GameServerGroups"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CompleteLifecycleAction",
      "autoscaling:ResumeProcesses",
      "autoscaling:EnterStandby",
      "autoscaling:SetInstanceProtection",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:SuspendProcesses",
      "autoscaling:DetachInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/GameLift" : "GameServerGroups"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "autoscaling:DescribeAutoScalingGroups",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "sns:Publish",
    "Resource" : [
      "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
      "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
    ]
  },
},

```

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

GlobalAcceleratorFullAccess

GlobalAcceleratorFullAccess es una [política administrada por AWS](#) que: permite a los usuarios de GlobalAccelerator el acceso total a todas las API

Uso de la política

Puede asociar GlobalAcceleratorFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2018 a las 02:44 UTC
- Hora de edición: 4 de diciembre de 2020, 19:17 UTC

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

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

GlobalAcceleratorReadOnlyAccess

GlobalAcceleratorReadOnlyAccess es una [política administrada por AWS](#) que: permite a los usuarios de GlobalAccelerator acceder a las API de solo lectura

Uso de la política

Puede asociar GlobalAcceleratorReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2018 a las 02:41 UTC
- Hora de edición: 27 de noviembre de 2018 a las 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

GreengrassOTAUpdateArtifactAccess

GreengrassOTAUpdateArtifactAccess es una [política administrada por AWS](#) que: proporciona acceso de lectura a los artefactos de actualización OTA de Greengrass en todas las regiones de Greengrass

Uso de la política

Puede asociar `GreengrassOTAUpdateArtifactAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de noviembre de 2017 a las 18:11 UTC
- Hora de edición: 18 de diciembre de 2018 a las 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

GroundTruthSyntheticConsoleFullAccess

GroundTruthSyntheticConsoleFullAccess es una [política administrada por AWS](#) que concede los permisos necesarios para utilizar todas las características de la consola sintética SageMaker Ground Truth.

Uso de la política

Puede asociar GroundTruthSyntheticConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de agosto de 2022 a las 15:58 UTC
- Hora de edición: 25 de agosto de 2022 a las 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "sagemaker-groundtruth-synthetic:*",
      "s3:ListBucket"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

GroundTruthSyntheticConsoleReadOnlyAccess

GroundTruthSyntheticConsoleReadOnlyAccess es una [política administrada por AWS](#) que: concede acceso de solo lectura a Sagemaker Ground Truth Synthetic a través de la AWS Management Console.

Uso de la política

Puede asociar GroundTruthSyntheticConsoleReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 25 de agosto de 2022 a las 15:58 UTC
- Hora de edición: 25 de agosto de 2022 a las 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

Health_OrganizationsServiceRolePolicy

Health_OrganizationsServiceRolePolicy es una [política administrada por AWS](#) que: otorga la Política de AWS Health para habilitar la característica Organizational View

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de diciembre de 2019 a las 13:28 UTC
- Hora editada: 6 de febrero de 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IAMAccessAdvisorReadOnly

IAMAccessAdvisorReadOnly es una [política administrada por AWS](#) que: otorga acceso para leer toda la información de acceso que brinda el asesor de acceso de IAM, como la información del último servicio al que se accedió.

Uso de la política

Puede asociar IAMAccessAdvisorReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 21 de junio de 2019 a las 19:33 UTC
- Hora de edición: 21 de junio de 2019 a las 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles",
      "iam:ListUsers",
      "iam:ListGroups",
      "iam:ListPolicies",
      "iam:ListPoliciesGrantingServiceAccess",
      "iam:GenerateServiceLastAccessedDetails",
      "iam:GenerateOrganizationsAccessReport",
      "iam:GenerateCredentialReport",
      "iam:GetRole",
      "iam:GetPolicy",
      "iam:GetServiceLastAccessedDetails",
      "iam:GetServiceLastAccessedDetailsWithEntities",
      "iam:GetOrganizationsAccessReport",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribePolicy",
      "organizations:ListChildren",
      "organizations:ListParents",
      "organizations:ListPoliciesForTarget",
      "organizations:ListRoots",
      "organizations:ListPolicies",
      "organizations:ListTargetsForPolicy"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IAMAccessAnalyzerFullAccess

IAMAccessAnalyzerFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a IAM Access Analyzer

Uso de la política

Puede asociar IAMAccessAnalyzerFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de diciembre de 2019 a las 17:12 UTC
- Hora de edición: 2 de diciembre de 2019 a las 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:ListAccounts",
      "organizations:ListAccountsForParent",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListChildren",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListOrganizationalUnitsForParent",
      "organizations:ListParents",
      "organizations:ListRoots"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IAMAccessAnalyzerReadOnlyAccess

IAMAccessAnalyzerReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a los recursos de IAM Access Analyzer

Uso de la política

Puede asociar `IAMAccessAnalyzerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 2 de diciembre de 2019 a las 17:12 UTC
- Hora editada: 27 de noviembre de 2023, 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IAMFullAccess

IAMFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a la IAM a través de la AWS Management Console.

Uso de la política

Puede asociar IAMFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 21 de junio de 2019 a las 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:*",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribePolicy",
      "organizations:ListChildren",
      "organizations:ListParents",
      "organizations:ListPoliciesForTarget",
      "organizations:ListRoots",
      "organizations:ListPolicies",
      "organizations:ListTargetsForPolicy"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IAMReadOnlyAccess

IAMReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a IAM a través de la AWS Management Console.

Uso de la política

Puede asociar IAMReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 25 de enero de 2018 a las 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)

- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IAMSelfManageServiceSpecificCredentials

IAMSelfManageServiceSpecificCredentials es una [política administrada por AWS](#) que: permite a un usuario de IAM gestionar sus propias credenciales específicas de servicio.

Uso de la política

Puede asociar IAMSelfManageServiceSpecificCredentials a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de diciembre de 2016 a las 17:25 UTC
- Hora de edición: 22 de diciembre de 2016 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Action" : [
  "iam:CreateServiceSpecificCredential",
  "iam:ListServiceSpecificCredentials",
  "iam:UpdateServiceSpecificCredential",
  "iam>DeleteServiceSpecificCredential",
  "iam:ResetServiceSpecificCredential"
],
"Resource" : "arn:aws:iam::*:user/${aws:username}"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IAMUserChangePassword

IAMUserChangePassword es una [política administrada por AWS](#) que: proporciona a un usuario de IAM la posibilidad de cambiar su propia contraseña.

Uso de la política

Puede asociar IAMUserChangePassword a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 15 de noviembre de 2016 a las 00:25 UTC
- Hora de edición: 15 de noviembre de 2016 a las 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IAMUserSSHKeys

IAMUserSSHKeys es una [política administrada por AWS](#) que: proporciona a un usuario de IAM la posibilidad de gestionar sus propias claves SSH.

Uso de la política

Puede asociar IAMUserSSHKeys a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de julio de 2015 a las 17:08 UTC
- Hora de edición: 9 de julio de 2015 a las 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IVSFullAccess

IVSFullAccesses una [política AWS gestionada](#) que: proporciona acceso completo al Servicio de vídeo interactivo (IVS). También incluye permisos para los servicios dependientes, necesarios para el acceso completo a la consola ivs.

Uso de la política

Puede asociar IVSFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 13 de diciembre de 2023 a las 21:20 UTC
- Hora editada: 13 de diciembre de 2023 a las 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

IVSReadOnlyAccess

IVSReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a las API de transmisión en tiempo real y baja latencia de IVS

Uso de la política

Puede asociar IVSReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS

- Hora de creación: 5 de diciembre de 2023 a las 18:00 UTC
- Hora editada: 16 de febrero de 2024 a las 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

IVSRecordToS3

IVSRecordToS3 es una [política administrada por AWS](#) que: brinda un rol vinculado a un servicio para realizar PutObject de S3 para grabar transmisiones en vivo de IVS

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de diciembre de 2020 a las 00:10 UTC
- Hora de edición: 5 de diciembre de 2020 a las 00:10 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

KafkaConnectServiceRolePolicy

KafkaConnectServiceRolePolicy es una [política administrada por AWS](#) que: concede a Kafka Connect permiso para gestionar los recursos de AWS en su nombre.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de septiembre de 2021 a las 13:12 UTC
- Hora de edición: 7 de septiembre de 2021 a las 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonMSKConnectManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonMSKConnectManaged"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2>DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMSKConnectManaged" : "true"
        }
      }
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

KafkaServiceRolePolicy

KafkaServiceRolePolicy es una [política administrada por AWS](#) que: otorga una política de roles vinculados a un servicio de IAM para Kafka.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2018 a las 23:31 UTC
- Hora de edición: 28 de abril de 2023 a las 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
"Action" : [
  "ec2:CreateNetworkInterface",
  "ec2:DescribeNetworkInterfaces",
  "ec2:CreateNetworkInterfacePermission",
  "ec2:AttachNetworkInterface",
  "ec2>DeleteNetworkInterface",
  "ec2:DetachNetworkInterface",
  "ec2:DescribeVpcEndpoints",
  "acm-pca:GetCertificateAuthorityCertificate",
  "secretsmanager:ListSecrets"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : "arn:*:ec2:*:*:subnet/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVpcEndpoints",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AWSMSKManaged" : "true"
    },
    "StringLike" : {
      "ec2:ResourceTag/ClusterArn" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetResourcePolicy",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager>DeleteResourcePolicy",
    "secretsmanager:DescribeSecret"
  ],
}
```

```
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
      }
    }
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

KeyspacesReplicationServiceRolePolicy

KeyspacesReplicationServiceRolePolicy es una [política administrada por AWS](#) que requiere permisos de Keyspaces para la replicación de datos entre regiones

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de mayo de 2023 a las 16:15 UTC
- Hora de edición: 2 de mayo de 2023 a las 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

LakeFormationDataAccessServiceRolePolicy

LakeFormationDataAccessServiceRolePolicy es una [política administrada por AWS](#) que: concede acceso temporal a los datos de los recursos de Lake Formation

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de junio de 2019 a las 20:46 UTC
- Hora editada: 6 de febrero de 2024 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

LexBotPolicy

LexBotPolicy es una [política administrada por AWS](#): para el caso de uso de AWS Lex Bot

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de febrero de 2017 a las 22:18 UTC
- Hora de edición: 13 de noviembre de 2019 a las 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "comprehend:DetectSentiment"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

LexChannelPolicy

LexChannelPolicy es una [política administrada por AWS](#) para: el caso de uso de AWS Lex Channel

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de febrero de 2017 a las 23:23 UTC
- Hora de edición: 17 de febrero de 2017 a las 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

LightsailExportAccess

LightsailExportAccess es una [política administrada por AWS](#) que: es una política de roles vinculados al servicio de AWS Lightsail que concede permisos para exportar recursos

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 28 de septiembre de 2018 a las 16:35 UTC

- Hora de edición: 15 de enero de 2022 a las 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/AWSServiceRoleForLightsail*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:CopyImage",
        "ec2:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

MediaConnectGatewayInstanceRolePolicy

MediaConnectGatewayInstanceRolePolicy es una [política administrada por AWS](#) que: concede permiso para registrar instancias de la Puerta de enlace de MediaConnect en una Puerta de enlace de MediaConnect.

Uso de la política

Puede asociar MediaConnectGatewayInstanceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 22 de marzo de 2023 a las 20:43 UTC
- Hora de edición: 22 de marzo de 2023 a las 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "MediaConnectGateway",
    "Effect" : "Allow",
    "Action" : [
      "mediaconnect:DiscoverGatewayPollEndpoint",
      "mediaconnect:PollGateway",
      "mediaconnect:SubmitGatewayStateChange"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

MediaPackageServiceRolePolicy

MediaPackageServiceRolePolicy es una [política administrada por AWS](#) que: permite que MediaPackage publique registros en CloudWatch

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de septiembre de 2020 a las 17:45 UTC

- Hora de edición: 18 de septiembre de 2020 a las 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

MemoryDBServiceRolePolicy

MemoryDBServiceRolePolicy es una [política administrada por AWS](#) que: permite que MemoryDB administre recursos AWS en su nombre, según lo necesite.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de agosto de 2021 a las 22:34 UTC
- Hora de edición: 18 de agosto de 2021 a las 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

MigrationHubDMSAccessServiceRolePolicy

MigrationHubDMSAccessServiceRolePolicy es una [política administrada por AWS](#) para: que Database Migration Service asuma un rol en la cuenta del cliente para llamar a Migration Hub

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 12 de junio de 2019 a las 17:50 UTC
- Hora de edición: 7 de octubre de 2019 a las 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : [  
      "mgh:ListMigrationTasks",  
      "mgh:NotifyApplicationState",  
      "mgh:DescribeApplicationState",  
      "mgh:GetHomeRegion"  
    ],  
    "Resource" : "*"    
  }  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

MigrationHubServiceRolePolicy

MigrationHubServiceRolePolicy es una [política administrada por AWS](#) que: permite que Migration Hub llame a Application Discovery Service en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de junio de 2019 a las 17:22 UTC
- Hora de edición: 6 de agosto de 2020 a las 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstanceAttribute"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

MigrationHubSMSAccessServiceRolePolicy

MigrationHubSMSAccessServiceRolePolicy es una [política administrada por AWS](#) que: se otorga para que el Servicio de Migración de Servidores asuma un rol en la cuenta del cliente para llamar a Migration Hub

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de junio de 2019 a las 18:30 UTC
- Hora de edición: 7 de octubre de 2019 a las 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

MonitronServiceRolePolicy

MonitronServiceRolePolicy es una [política administrada por AWS](#) para que: el rol vinculado a un servicio de AWS Monitron otorgue acceso a los recursos requeridos por los clientes.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de mayo de 2022 a las 19:22 UTC
- Hora de edición: 2 de mayo de 2022 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    ]
  }
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

NeptuneConsoleFullAccess

NeptuneConsoleFullAccess es una [política administrada por AWS](#) que: otorga acceso total para gestionar Amazon Neptune mediante la AWS Management Console. Tenga en cuenta que esta política también otorga acceso total para publicar sobre todos los temas de SNS de la cuenta. A su vez, concede permisos para crear y editar instancias de Amazon EC2 y configuraciones de VPC, y para ver y enumerar claves en Amazon KMS. Por último brinda acceso total a Amazon RDS. Para obtener más información, consulte <https://aws.amazon.com/neptune/faqs/>.

Uso de la política

Puede asociar NeptuneConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 19 de junio de 2018 a las 21:35 UTC

- Hora editada: 30 de noviembre de 2023 a las 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
```

```
"rds:CopyDBClusterParameterGroup",
"rds:CopyDBClusterSnapshot",
"rds:CopyDBParameterGroup",
"rds:CreateDBClusterParameterGroup",
"rds:CreateDBClusterSnapshot",
"rds:CreateDBParameterGroup",
"rds:CreateDBSubnetGroup",
"rds:CreateEventSubscription",
"rds>DeleteDBCluster",
"rds>DeleteDBClusterParameterGroup",
"rds>DeleteDBClusterSnapshot",
"rds>DeleteDBInstance",
"rds>DeleteDBParameterGroup",
"rds>DeleteDBSubnetGroup",
"rds>DeleteEventSubscription",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
```

```

    "rds:ModifyDBInstance",
    "rds:ModifyDBParameterGroup",
    "rds:ModifyDBSubnetGroup",
    "rds:ModifyEventSubscription",
    "rds:PromoteReadReplicaDBCluster",
    "rds:RebootDBInstance",
    "rds:RemoveRoleFromDBCluster",
    "rds:RemoveSourceIdentifierFromSubscription",
    "rds:RemoveTagsFromResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "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"
    }
  }
}
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

NeptuneFullAccess

NeptuneFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a Amazon Neptune. Tenga en cuenta que esta política también otorga acceso total a las publicaciones sobre todos los temas de SNS de la cuenta, y brinda acceso total a Amazon RDS. Para obtener más información, consulte <https://aws.amazon.com/neptune/faqs/>.

Uso de la política

Puede asociar NeptuneFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de mayo de 2018 a las 19:17 UTC
- Hora editada: 22 de enero de 2024 a las 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
```



```

    "arn:aws:rds:*:*:*"
  ],
  "Condition" : {
    "StringEquals" : {
      "rds:DatabaseEngine" : [
        "graphdb",
        "neptune"
      ]
    }
  }
},
{
  "Sid" : "AllowManagementPermissionsForRDS",
  "Effect" : "Allow",
  "Action" : [
    "rds:AddRoleToDBCluster",
    "rds:AddSourceIdentifierToSubscription",
    "rds:AddTagsToResource",
    "rds:ApplyPendingMaintenanceAction",
    "rds:CopyDBClusterParameterGroup",
    "rds:CopyDBClusterSnapshot",
    "rds:CopyDBParameterGroup",
    "rds>CreateDBClusterEndpoint",
    "rds>CreateDBClusterParameterGroup",
    "rds>CreateDBClusterSnapshot",
    "rds>CreateDBParameterGroup",
    "rds>CreateDBSubnetGroup",
    "rds>CreateEventSubscription",
    "rds>CreateGlobalCluster",
    "rds>DeleteDBCluster",
    "rds>DeleteDBClusterEndpoint",
    "rds>DeleteDBClusterParameterGroup",
    "rds>DeleteDBClusterSnapshot",
    "rds>DeleteDBInstance",
    "rds>DeleteDBParameterGroup",
    "rds>DeleteDBSubnetGroup",
    "rds>DeleteEventSubscription",
    "rds>DeleteGlobalCluster",
    "rds:DescribeDBClusterEndpoints",
    "rds:DescribeAccountAttributes",
    "rds:DescribeCertificates",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBClusterSnapshotAttributes",

```

```
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:FailoverGlobalCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterEndpoint",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
"rds:ModifyGlobalCluster",
"rds:PromoteReadReplicaDBCluster",
"rds:RebootDBInstance",
"rds:RemoveFromGlobalCluster",
"rds:RemoveRoleFromDBCluster",
"rds:RemoveSourceIdentifierFromSubscription",
"rds:RemoveTagsFromResource",
"rds:ResetDBClusterParameterGroup",
"rds:ResetDBParameterGroup",
"rds:RestoreDBClusterFromSnapshot",
"rds:RestoreDBClusterToPointInTime",
"rds:StartDBCluster",
"rds:StopDBCluster"
```

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

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

NeptuneGraphReadOnlyAccess

NeptuneGraphReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a todos los recursos de Amazon Neptune Analytics junto con permisos de solo lectura para los servicios dependientes.

Uso de la política

Puede asociar `NeptuneGraphReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de noviembre de 2023 a las 07:32 UTC
- Hora editada: 30 de noviembre de 2023 a las 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
```

```
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeAvailabilityZones"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForKMS",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
  ]
}
]
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

NeptuneReadOnlyAccess

NeptuneReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Amazon Neptune. Tenga en cuenta que esta política también concede acceso a los recursos de Amazon RDS. Para obtener más información, consulte <https://aws.amazon.com/neptune/faqs/>.

Uso de la política

Puede asociar NeptuneReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de mayo de 2018 a las 19:16 UTC
- Hora editada: 22 de enero de 2024 a las 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ],
  {
```



```

    "Sid" : "AllowReadOnlyPermissionsForEC2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForKMS",
    "Effect" : "Allow",
    "Action" : [
      "kms:ListKeys",
      "kms:ListRetirableGrants",
      "kms:ListAliases",
      "kms:ListKeyPolicies"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
      "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
    ]
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
    "Effect" : "Allow",
    "Action" : [
      "neptune-db:Read*",
      "neptune-db:Get*",
      "neptune-db:List*"
    ],
  },

```

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

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

NetworkAdministrator

NetworkAdministrator es una [política administrada por AWS](#) que: otorga permisos de acceso total a los servicios y acciones de AWS necesarios para instalar y configurar los recursos de AWS de la red.

Uso de la política

Puede asociar NetworkAdministrator a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:31 UTC
- Hora de edición: 16 de septiembre de 2021 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

OAMFullAccess

OAMFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a CloudWatch Observability Access Manager

Uso de la política

Puede asociar `OAMFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2022 a las 13:38 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

OAMReadOnlyAccess

OAMReadOnlyAccess es una [política administrada por AWS](#) que: otorga acceso de solo lectura a CloudWatch Observability Access Manager

Uso de la política

Puede asociar OAMReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2022 a las 13:29 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

PartnerCentralAccountManagementUserRoleAssociation

PartnerCentralAccountManagementUserRoleAssociation es una [política administrada por AWS](#) que: proporciona acceso para asociar y disociar a los usuarios centrales de los socios con roles de IAM

Uso de la política

Puede asociar PartnerCentralAccountManagementUserRoleAssociation a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 10 de noviembre de 2023 a las 02:03 UTC
- Hora de edición: 10 de noviembre de 2023 a las 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "partnercentral-account-management:AssociatePartnerUser",
        "partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

PowerUserAccess

PowerUserAccess es una [política administrada por AWS](#) que: brinda acceso total a los servicios y recursos de AWS, pero no permite la administración de usuarios y grupos.

Uso de la política

Puede asociar PowerUserAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de julio de 2023 a las 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

QuickSightAccessForS3StorageManagementAnalyticsReadOnly es una [política administrada por AWS](#) que: el equipo de QuickSight utiliza para acceder a los datos de los clientes generados por S3 Storage Management Analytics.

Uso de la política

Puede asociar QuickSightAccessForS3StorageManagementAnalyticsReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de junio de 2017 a las 18:18 UTC
- Hora de edición: 8 de octubre de 2019 a las 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::s3-analytics-export-shared-*"
      ]
    },
    {
      "Action" : [
        "s3:GetAnalyticsConfiguration",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```



```
]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

RDSCloudHsmAuthorizationRole

RDSCloudHsmAuthorizationRole es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio de Amazon RDS.

Uso de la política

Puede asociar RDSCloudHsmAuthorizationRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 26 de septiembre de 2019 a las 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ReadOnlyAccess

ReadOnlyAccesses una [política AWS gestionada](#) que: proporciona acceso de solo lectura a AWS los servicios y recursos.

Uso de la política

Puede asociar ReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora editada: 5 de febrero de 2024 a las 15:00 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Versión de la política

Versión de la política: v111 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "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:GetEntityTypeTypes",
"frauddetector:GetEvent",
"frauddetector:GetEventPredictionMetadata",
"frauddetector:GetEventTypes",
"frauddetector:GetExternalModels",
"frauddetector:GetKMSEncryptionKey",
"frauddetector:GetLabels",
"frauddetector:GetListElements",
"frauddetector:GetListsMetadata",
"frauddetector:GetModels",
"frauddetector:GetModelVersion",
"frauddetector:GetOutcomes",
"frauddetector:GetRules",
"frauddetector:GetVariables",
"frauddetector:ListEventPredictions",
"frauddetector:ListTagsForResource",
"freertos:Describe*",
"freertos:List*",
"freetier:GetFreeTierAlertPreference",
"freetier:GetFreeTierUsage",
"fsx:Describe*",
"fsx:List*",
"gamelift:Describe*",
"gamelift:Get*",
"gamelift:List*",
"gamelift:ResolveAlias",
"gamelift:Search*",
"glacier:Describe*",
"glacier:Get*",
"glacier:List*",
"globalaccelerator:Describe*",
"globalaccelerator:List*",
"glue:BatchGetCrawlers",
"glue:BatchGetDevEndpoints",
"glue:BatchGetJobs",
```

```
"glue:BatchGetPartition",
"glue:BatchGetTriggers",
"glue:BatchGetWorkflows",
"glue:CheckSchemaVersionValidity",
"glue:GetCatalogImportStatus",
"glue:GetClassifier",
"glue:GetClassifiers",
"glue:GetCrawler",
"glue:GetCrawlerMetrics",
"glue:GetCrawlers",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDataflowGraph",
"glue:GetDevEndpoint",
"glue:GetDevEndpoints",
"glue:GetJob",
"glue:GetJobBookmark",
"glue:GetJobRun",
"glue:GetJobRuns",
"glue:GetJobs",
"glue:GetMapping",
"glue:GetMLTaskRun",
"glue:GetMLTaskRuns",
"glue:GetMLTransform",
"glue:GetMLTransforms",
"glue:GetPartition",
"glue:GetPartitions",
"glue:GetPlan",
"glue:GetRegistry",
"glue:GetResourcePolicy",
"glue:GetSchema",
"glue:GetSchemaByDefinition",
"glue:GetSchemaVersion",
"glue:GetSchemaVersionsDiff",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTables",
"glue:GetTableVersion",
"glue:GetTableVersions",
"glue:GetTags",
"glue:GetTrigger",
"glue:GetTriggers",
```

```
"glue:GetUserDefinedFunction",
"glue:GetUserDefinedFunctions",
"glue:GetWorkflow",
"glue:GetWorkflowRun",
"glue:GetWorkflowRunProperties",
"glue:GetWorkflowRuns",
"glue:ListCrawlers",
"glue:ListCrawls",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
"glue:ListRegistries",
"glue:ListSchemas",
"glue:ListSchemaVersions",
"glue:ListTriggers",
"glue:ListWorkflows",
"glue:QuerySchemaVersionMetadata",
"glue:SearchTables",
"grafana:DescribeWorkspace",
"grafana:DescribeWorkspaceAuthentication",
"grafana:DescribeWorkspaceConfiguration",
"grafana:ListPermissions",
"grafana:ListTagsForResource",
"grafana:ListVersions",
"grafana:ListWorkspaces",
"greengrass:DescribeComponent",
"greengrass:Get*",
"greengrass:List*",
"groundstation:DescribeContact",
"groundstation:GetConfig",
"groundstation:GetDataflowEndpointGroup",
"groundstation:GetMinuteUsage",
"groundstation:GetMissionProfile",
"groundstation:GetSatellite",
"groundstation:ListConfigs",
"groundstation:ListContacts",
"groundstation:ListDataflowEndpointGroups",
"groundstation:ListGroundStations",
"groundstation:ListMissionProfiles",
"groundstation:ListSatellites",
"groundstation:ListTagsForResource",
"guardduty:Describe*",
"guardduty:Get*",
"guardduty:List*",
```

```
"health:Describe*",
"healthlake:DescribeFHIRDatastore",
"healthlake:DescribeFHIRExportJob",
"healthlake:DescribeFHIRImportJob",
"healthlake:GetCapabilities",
"healthlake:ListFHIRDatastores",
"healthlake:ListFHIRExportJobs",
"healthlake:ListFHIRImportJobs",
"healthlake:ListTagsForResource",
"healthlake:ReadResource",
"healthlake:SearchWithGet",
"healthlake:SearchWithPost",
"iam:Generate*",
"iam:Get*",
"iam:List*",
"iam:Simulate*",
"identity-sync:GetSyncProfile",
"identity-sync:GetSyncTarget",
"identity-sync:ListSyncFilters",
"identitystore-auth:BatchGetSession",
"identitystore-auth:ListSessions",
"identitystore:DescribeGroup",
"identitystore:DescribeGroupMembership",
"identitystore:DescribeUser",
"identitystore:GetGroupId",
"identitystore:GetGroupMembershipId",
"identitystore:GetUserId",
"identitystore:IsMemberInGroups",
"identitystore:ListGroupMemberships",
"identitystore:ListGroupMembershipsForMember",
"identitystore:ListGroups",
"identitystore:ListUsers",
"imagebuilder:Get*",
"imagebuilder:List*",
"importexport:Get*",
"importexport:List*",
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
"inspector2:BatchGetAccountStatus",
"inspector2:BatchGetFreeTrialInfo",
"inspector2:DescribeOrganizationConfiguration",
"inspector2:GetDelegatedAdminAccount",
```

```
"inspector2:GetFindingsReportStatus",
"inspector2:GetMember",
"inspector2:ListAccountPermissions",
"inspector2:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListMembers",
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"internetmonitor:GetHealthEvent",
"internetmonitor:GetMonitor",
"internetmonitor:ListHealthEvents",
"internetmonitor:ListMonitors",
"internetmonitor:ListTagsForResource",
" invoicing:GetInvoiceEmailDeliveryPreferences",
" invoicing:GetInvoicePDF",
" invoicing:ListInvoiceSummaries",
" iot:Describe*",
" iot:Get*",
" iot:List*",
" iot1click:DescribeDevice",
" iot1click:DescribePlacement",
" iot1click:DescribeProject",
" iot1click:GetDeviceMethods",
" iot1click:GetDevicesInPlacement",
" iot1click:ListDeviceEvents",
" iot1click:ListDevices",
" iot1click:ListPlacements",
" iot1click:ListProjects",
" iot1click:ListTagsForResource",
" iotanalytics:Describe*",
" iotanalytics:Get*",
" iotanalytics:List*",
" iotanalytics:SampleChannelData",
" iotevents:DescribeAlarm",
" iotevents:DescribeAlarmModel",
" iotevents:DescribeDetector",
" iotevents:DescribeDetectorModel",
" iotevents:DescribeInput",
" iotevents:DescribeLoggingOptions",
" iotevents:ListAlarmModels",
```



```
"iotevents:ListAlarmModelVersions",
"iotevents:ListAlarms",
"iotevents:ListDetectorModels",
"iotevents:ListDetectorModelVersions",
"iotevents:ListDetectors",
"iotevents:ListInputs",
"iotevents:ListTagsForResource",
"iotfleethub:DescribeApplication",
"iotfleethub:ListApplications",
"iotfleetwise:GetCampaign",
"iotfleetwise:GetDecoderManifest",
"iotfleetwise:GetFleet",
"iotfleetwise:GetLoggingOptions",
"iotfleetwise:GetModelManifest",
"iotfleetwise:GetRegisterAccountStatus",
"iotfleetwise:GetSignalCatalog",
"iotfleetwise:GetVehicle",
"iotfleetwise:GetVehicleStatus",
"iotfleetwise:ListCampaigns",
"iotfleetwise:ListDecoderManifestNetworkInterfaces",
"iotfleetwise:ListDecoderManifests",
"iotfleetwise:ListDecoderManifestSignals",
"iotfleetwise:ListFleets",
"iotfleetwise:ListFleetsForVehicle",
"iotfleetwise:ListModelManifestNodes",
"iotfleetwise:ListModelManifests",
"iotfleetwise:ListSignalCatalogNodes",
"iotfleetwise:ListSignalCatalogs",
"iotfleetwise:ListTagsForResource",
"iotfleetwise:ListVehicles",
"iotfleetwise:ListVehiclesInFleet",
"iotroborunner:GetDestination",
"iotroborunner:GetSite",
"iotroborunner:GetWorker",
"iotroborunner:GetWorkerFleet",
"iotroborunner:ListDestinations",
"iotroborunner:ListSites",
"iotroborunner:ListWorkerFleets",
"iotroborunner:ListWorkers",
"iotsitewise:Describe*",
"iotsitewise:Get*",
"iotsitewise:List*",
"iotwireless:GetDestination",
"iotwireless:GetDeviceProfile",
```

```
"iotwireless:GetEventConfigurationByResourceTypes",
"iotwireless:GetFuotaTask",
"iotwireless:GetLogLevelsByResourceTypes",
"iotwireless:GetMulticastGroup",
"iotwireless:GetMulticastGroupSession",
"iotwireless:GetNetworkAnalyzerConfiguration",
"iotwireless:GetPartnerAccount",
"iotwireless:GetPosition",
"iotwireless:GetPositionConfiguration",
"iotwireless:GetPositionEstimate",
"iotwireless:GetResourceEventConfiguration",
"iotwireless:GetResourceLogLevel",
"iotwireless:GetResourcePosition",
"iotwireless:GetServiceEndpoint",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessDeviceImportTask",
"iotwireless:GetWirelessDeviceStatistics",
"iotwireless:GetWirelessGateway",
"iotwireless:GetWirelessGatewayCertificate",
"iotwireless:GetWirelessGatewayFirmwareInformation",
"iotwireless:GetWirelessGatewayStatistics",
"iotwireless:GetWirelessGatewayTask",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListDestinations",
"iotwireless:ListDeviceProfiles",
"iotwireless:ListDevicesForWirelessDeviceImportTask",
"iotwireless:ListEventConfigurations",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListMulticastGroupsByFuotaTask",
"iotwireless:ListNetworkAnalyzerConfigurations",
"iotwireless:ListPartnerAccounts",
"iotwireless:ListPositionConfigurations",
"iotwireless:ListQueuedMessages",
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDeviceImportTasks",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGateways",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:BatchGetChannel",
"ivs:GetChannel",
"ivs:GetPlaybackKeyPair",
```

```
"ivs:GetRecordingConfiguration",
"ivs:GetStreamSession",
"ivs:ListChannels",
"ivs:ListPlaybackKeyPairs",
"ivs:ListRecordingConfigurations",
"ivs:ListStreams",
"ivs:ListStreamSessions",
"ivs:ListTagsForResource",
"ivschat:GetLoggingConfiguration",
"ivschat:GetRoom",
"ivschat:ListLoggingConfigurations",
"ivschat:ListRooms",
"ivschat:ListTagsForResource",
"kafka:Describe*",
"kafka:DescribeCluster",
"kafka:DescribeClusterOperation",
"kafka:DescribeClusterV2",
"kafka:DescribeConfiguration",
"kafka:DescribeConfigurationRevision",
"kafka:Get*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafka:ListClusterOperations",
"kafka:ListClusters",
"kafka:ListClustersV2",
"kafka:ListConfigurationRevisions",
"kafka:ListConfigurations",
"kafka:ListKafkaVersions",
"kafka:ListNodes",
"kafka:ListTagsForResource",
"kafkaconnect:DescribeConnector",
"kafkaconnect:DescribeCustomPlugin",
"kafkaconnect:DescribeWorkerConfiguration",
"kafkaconnect:ListConnectors",
"kafkaconnect:ListCustomPlugins",
"kafkaconnect:ListWorkerConfigurations",
"kendra:BatchGetDocumentStatus",
"kendra:DescribeDataSource",
"kendra:DescribeExperience",
"kendra:DescribeFaq",
"kendra:DescribeIndex",
"kendra:DescribePrincipalMapping",
"kendra:DescribeQuerySuggestionsBlockList",
```

```
"kendra:DescribeQuerySuggestionsConfig",
"kendra:DescribeThesaurus",
"kendra:GetQuerySuggestions",
"kendra:GetSnapshots",
"kendra:ListDataSources",
"kendra:ListDataSourceSyncJobs",
"kendra:ListEntityPersonas",
"kendra:ListExperienceEntities",
"kendra:ListExperiences",
"kendra:ListFaqs",
"kendra:ListGroupsOlderThanOrderingId",
"kendra:ListIndices",
"kendra:ListQuerySuggestionsBlockLists",
"kendra:ListTagsForResource",
"kendra:ListThesauri",
"kendra:Query",
"kinesis:Describe*",
"kinesis:Get*",
"kinesis:List*",
"kinesisanalytics:Describe*",
"kinesisanalytics:Discover*",
"kinesisanalytics:Get*",
"kinesisanalytics:List*",
"kinesisvideo:Describe*",
"kinesisvideo:Get*",
"kinesisvideo:List*",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lakeformation:DescribeResource",
"lakeformation:GetDataCellsFilter",
"lakeformation:GetDataLakeSettings",
"lakeformation:GetEffectivePermissionsForPath",
"lakeformation:GetLfTag",
"lakeformation:GetResourceLfTags",
"lakeformation:ListDataCellsFilter",
"lakeformation:ListLfTags",
"lakeformation:ListPermissions",
"lakeformation:ListResources",
"lakeformation:ListTableStorageOptimizers",
"lakeformation:SearchDatabasesByLfTags",
"lakeformation:SearchTablesByLfTags",
"lambda:Get*",
"lambda:List*",
```

```
"launchwizard:DescribeAdditionalNode",
"launchwizard:DescribeProvisionedApp",
"launchwizard:DescribeProvisioningEvents",
"launchwizard:DescribeSettingsSet",
"launchwizard:GetDeployment",
"launchwizard:GetInfrastructureSuggestion",
"launchwizard:GetIpAddress",
"launchwizard:GetResourceCostEstimate",
"launchwizard:GetResourceRecommendation",
"launchwizard:GetSettingsSet",
"launchwizard:GetWorkload",
"launchwizard:GetWorkloadAsset",
"launchwizard:GetWorkloadAssets",
"launchwizard>ListAdditionalNodes",
"launchwizard>ListAllowedResources",
"launchwizard>ListDeploymentEvents",
"launchwizard>ListDeployments",
"launchwizard>ListProvisionedApps",
"launchwizard>ListResourceCostEstimates",
"launchwizard>ListSettingsSets",
"launchwizard>ListWorkloadDeploymentOptions",
"launchwizard>ListWorkloadDeploymentPatterns",
"launchwizard>ListWorkloads",
"lex:DescribeBot",
"lex:DescribeBotAlias",
"lex:DescribeBotChannel",
"lex:DescribeBotLocale",
"lex:DescribeBotVersion",
"lex:DescribeExport",
"lex:DescribeImport",
"lex:DescribeIntent",
"lex:DescribeResourcePolicy",
"lex:DescribeSlot",
"lex:DescribeSlotType",
"lex:Get*",
"lex>ListBotAliases",
"lex>ListBotChannels",
"lex>ListBotLocales",
"lex>ListBots",
"lex>ListBotVersions",
"lex>ListBuiltInIntents",
"lex>ListBuiltInSlotTypes",
"lex>ListExports",
"lex>ListImports",
```

```
"lex:ListIntents",
"lex:ListSlots",
"lex:ListSlotTypes",
"lex:ListTagsForResource",
"license-manager:Get*",
"license-manager:List*",
"lightsail:GetActiveNames",
"lightsail:GetAlarms",
"lightsail:GetAutoSnapshots",
"lightsail:GetBlueprints",
"lightsail:GetBucketAccessKeys",
"lightsail:GetBucketBundles",
"lightsail:GetBucketMetricData",
"lightsail:GetBuckets",
"lightsail:GetBundles",
"lightsail:GetCertificates",
"lightsail:GetCloudFormationStackRecords",
"lightsail:GetContainerAPIMetadata",
"lightsail:GetContainerImages",
"lightsail:GetContainerServiceDeployments",
"lightsail:GetContainerServiceMetricData",
"lightsail:GetContainerServicePowers",
"lightsail:GetContainerServices",
"lightsail:GetDisk",
"lightsail:GetDisks",
"lightsail:GetDiskSnapshot",
"lightsail:GetDiskSnapshots",
"lightsail:GetDistributionBundles",
"lightsail:GetDistributionLatestCacheReset",
"lightsail:GetDistributionMetricData",
"lightsail:GetDistributions",
"lightsail:GetDomain",
"lightsail:GetDomains",
"lightsail:GetExportSnapshotRecords",
"lightsail:GetInstance",
"lightsail:GetInstanceMetricData",
"lightsail:GetInstancePortStates",
"lightsail:GetInstances",
"lightsail:GetInstanceSnapshot",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstanceState",
"lightsail:GetKeyPair",
"lightsail:GetKeyPairs",
"lightsail:GetLoadBalancer",
```

```
"lightsail:GetLoadBalancerMetricData",
"lightsail:GetLoadBalancers",
"lightsail:GetLoadBalancerTlsCertificates",
"lightsail:GetOperation",
"lightsail:GetOperations",
"lightsail:GetOperationsForResource",
"lightsail:GetRegions",
"lightsail:GetRelationalDatabase",
"lightsail:GetRelationalDatabaseBlueprints",
"lightsail:GetRelationalDatabaseBundles",
"lightsail:GetRelationalDatabaseEvents",
"lightsail:GetRelationalDatabaseLogEvents",
"lightsail:GetRelationalDatabaseLogStreams",
"lightsail:GetRelationalDatabaseMetricData",
"lightsail:GetRelationalDatabaseParameters",
"lightsail:GetRelationalDatabases",
"lightsail:GetRelationalDatabaseSnapshot",
"lightsail:GetRelationalDatabaseSnapshots",
"lightsail:GetStaticIp",
"lightsail:GetStaticIps",
"lightsail:Is*",
"logs:Describe*",
"logs:FilterLogEvents",
"logs:Get*",
"logs:ListAnomalies",
"logs:ListLogAnomalyDetectors",
"logs:ListLogDeliveries",
"logs:ListTagsForResource",
"logs:ListTagsLogGroup",
"logs:StartLiveTail",
"logs:StartQuery",
"logs:StopLiveTail",
"logs:StopQuery",
"logs:TestMetricFilter",
"lookoutequipment:DescribeDataIngestionJob",
"lookoutequipment:DescribeDataset",
"lookoutequipment:DescribeInferenceScheduler",
"lookoutequipment:DescribeLabel",
"lookoutequipment:DescribeLabelGroup",
"lookoutequipment:DescribeModel",
"lookoutequipment:DescribeModelVersion",
"lookoutequipment:DescribeResourcePolicy",
"lookoutequipment:DescribeRetrainingScheduler",
"lookoutequipment:ListDataIngestionJobs",
```

```
"lookoutequipment:ListDatasets",
"lookoutequipment:ListInferenceEvents",
"lookoutequipment:ListInferenceExecutions",
"lookoutequipment:ListInferenceSchedulers",
"lookoutequipment:ListLabelGroups",
"lookoutequipment:ListLabels",
"lookoutequipment:ListModels",
"lookoutequipment:ListModelVersions",
"lookoutequipment:ListRetrainingSchedulers",
"lookoutequipment:ListSensorStatistics",
"lookoutequipment:ListTagsForResource",
"lookoutmetrics:Describe*",
"lookoutmetrics:Get*",
"lookoutmetrics:List*",
"lookoutvision:DescribeDataset",
"lookoutvision:DescribeModel",
"lookoutvision:DescribeModelPackagingJob",
"lookoutvision:DescribeProject",
"lookoutvision:ListDatasetEntries",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"lookoutvision:ListTagsForResource",
"m2:GetApplication",
"m2:GetApplicationVersion",
"m2:GetBatchJobExecution",
"m2:GetDataSetDetails",
"m2:GetDataSetImportTask",
"m2:GetDeployment",
"m2:GetEnvironment",
"m2:ListApplications",
"m2:ListApplicationVersions",
"m2:ListBatchJobDefinitions",
"m2:ListBatchJobExecutions",
"m2:ListDataSetImportHistory",
"m2:ListDataSets",
"m2:ListDeployments",
"m2:ListEngineVersions",
"m2:ListEnvironments",
"m2:ListTagsForResource",
"machinelearning:Describe*",
"machinelearning:Get*",
"macie2:BatchGetCustomDataIdentifiers",
"macie2:DescribeBuckets",
```



```
"macie2:DescribeClassificationJob",
"macie2:DescribeOrganizationConfiguration",
"macie2:GetAdministratorAccount",
"macie2:GetAllowList",
"macie2:GetAutomatedDiscoveryConfiguration",
"macie2:GetBucketStatistics",
"macie2:GetClassificationExportConfiguration",
"macie2:GetClassificationScope",
"macie2:GetCustomDataIdentifier",
"macie2:GetFindings",
"macie2:GetFindingsFilter",
"macie2:GetFindingsPublicationConfiguration",
"macie2:GetFindingStatistics",
"macie2:GetInvitationsCount",
"macie2:GetMacieSession",
"macie2:GetMember",
"macie2:GetResourceProfile",
"macie2:GetRevealConfiguration",
"macie2:GetSensitiveDataOccurrencesAvailability",
"macie2:GetSensitivityInspectionTemplate",
"macie2:GetUsageStatistics",
"macie2:GetUsageTotals",
"macie2:ListAllowLists",
"macie2:ListClassificationJobs",
"macie2:ListClassificationScopes",
"macie2:ListCustomDataIdentifiers",
"macie2:ListFindings",
"macie2:ListFindingsFilters",
"macie2:ListInvitations",
"macie2:ListMembers",
"macie2:ListOrganizationAdminAccounts",
"macie2:ListResourceProfileArtifacts",
"macie2:ListResourceProfileDetections",
"macie2:ListSensitivityInspectionTemplates",
"macie2:ListTagsForResource",
"macie2:SearchResources",
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
"managedblockchain:GetNode",
"managedblockchain:GetProposal",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNetworks",
"managedblockchain:ListNodes",
```

```
"managedblockchain:ListProposals",
"managedblockchain:ListProposalVotes",
"managedblockchain:ListTagsForResource",
"mediaconnect:DescribeFlow",
"mediaconnect:DescribeOffering",
"mediaconnect:DescribeReservation",
"mediaconnect:ListEntitlements",
"mediaconnect:ListFlows",
"mediaconnect:ListOfferings",
"mediaconnect:ListReservations",
"mediaconnect:ListTagsForResource",
"mediaconvert:DescribeEndpoints",
"mediaconvert:Get*",
"mediaconvert:List*",
"medialive:DescribeChannel",
"medialive:DescribeInput",
"medialive:DescribeInputDevice",
"medialive:DescribeInputDeviceThumbnail",
"medialive:DescribeInputSecurityGroup",
"medialive:DescribeMultiplex",
"medialive:DescribeMultiplexProgram",
"medialive:DescribeOffering",
"medialive:DescribeReservation",
"medialive:DescribeSchedule",
"medialive:ListChannels",
"medialive:ListInputDevices",
"medialive:ListInputDeviceTransfers",
"medialive:ListInputs",
"medialive:ListInputSecurityGroups",
"medialive:ListMultiplexes",
"medialive:ListMultiplexPrograms",
"medialive:ListOfferings",
"medialive:ListReservations",
"medialive:ListTagsForResource",
"mediapackage-vod:Describe*",
"mediapackage-vod:List*",
"mediapackage:Describe*",
"mediapackage:List*",
"mediapackagev2:GetChannel",
"mediapackagev2:GetChannelGroup",
"mediapackagev2:GetChannelPolicy",
"mediapackagev2:GetHeadObject",
"mediapackagev2:GetObject",
"mediapackagev2:GetOriginEndpoint",
```

```
"mediapackagev2:GetOriginEndpointPolicy",
"mediapackagev2:ListChannelGroups",
"mediapackagev2:ListChannels",
"mediapackagev2:ListOriginEndpoints",
"mediapackagev2:ListTagsForResource",
"mediastore:DescribeContainer",
"mediastore:DescribeObject",
"mediastore:GetContainerPolicy",
"mediastore:GetCorsPolicy",
"mediastore:GetLifecyclePolicy",
"mediastore:GetMetricPolicy",
"mediastore:GetObject",
"mediastore:ListContainers",
"mediastore:ListItems",
"mediastore:ListTagsForResource",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeParameters",
"memorydb:ListTags",
"mgh:Describe*",
"mgh:GetHomeRegion",
"mgh:List*",
"mgn:DescribeJobLogItems",
"mgn:DescribeJobs",
"mgn:DescribeLaunchConfigurationTemplates",
"mgn:DescribeReplicationConfigurationTemplates",
"mgn:DescribeSourceServers",
"mgn:DescribeVcenterClients",
"mgn:GetLaunchConfiguration",
"mgn:GetReplicationConfiguration",
"mgn:ListApplications",
"mgn:ListSourceServerActions",
"mgn:ListTemplateActions",
"mgn:ListWaves",
"mobileanalytics:Get*",
"mobiletargeting:Get*",
"mobiletargeting:List*",
"monitron:GetProject",
"monitron:GetProjectAdminUser",
"monitron:ListProjects",
"monitron:ListTagsForResource",
"mq:Describe*",
"mq:List*",
"network-firewall:DescribeFirewall",
```

```
"network-firewall:DescribeFirewallPolicy",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:DescribeResourcePolicy",
"network-firewall:DescribeRuleGroup",
"network-firewall:DescribeRuleGroupMetadata",
"network-firewall:DescribeTLSInspectionConfiguration",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"network-firewall:ListRuleGroups",
"network-firewall:ListTagsForResource",
"network-firewall:ListTLSInspectionConfigurations",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetConnectAttachment",
"networkmanager:GetConnections",
"networkmanager:GetConnectPeer",
"networkmanager:GetConnectPeerAssociations",
"networkmanager:GetCoreNetwork",
"networkmanager:GetCoreNetworkChangeEvents",
"networkmanager:GetCoreNetworkChangeSet",
"networkmanager:GetCoreNetworkPolicy",
"networkmanager:GetCustomerGatewayAssociations",
"networkmanager:GetDevices",
"networkmanager:GetLinkAssociations",
"networkmanager:GetLinks",
"networkmanager:GetNetworkResourceCounts",
"networkmanager:GetNetworkResourceRelationships",
"networkmanager:GetNetworkResources",
"networkmanager:GetNetworkRoutes",
"networkmanager:GetNetworkTelemetry",
"networkmanager:GetResourcePolicy",
"networkmanager:GetRouteAnalysis",
"networkmanager:GetSites",
"networkmanager:GetSiteToSiteVpnAttachment",
"networkmanager:GetTransitGatewayConnectPeerAssociations",
"networkmanager:GetTransitGatewayPeering",
"networkmanager:GetTransitGatewayRegistrations",
"networkmanager:GetTransitGatewayRouteTableAttachment",
"networkmanager:GetVpcAttachment",
"networkmanager:ListAttachments",
"networkmanager:ListConnectPeers",
"networkmanager:ListCoreNetworkPolicyVersions",
"networkmanager:ListCoreNetworks",
"networkmanager:ListPeerings",
"networkmanager:ListTagsForResource",
```

```
"nimble:GetEula",
"nimble:GetFeatureMap",
"nimble:GetLaunchProfile",
"nimble:GetLaunchProfileDetails",
"nimble:GetLaunchProfileInitialization",
"nimble:GetLaunchProfileMember",
"nimble:GetStreamingImage",
"nimble:GetStreamingSession",
"nimble:GetStudio",
"nimble:GetStudioComponent",
"nimble:GetStudioMember",
"nimble:ListEulaAcceptances",
"nimble:ListEulas",
"nimble:ListLaunchProfileMembers",
"nimble:ListLaunchProfiles",
"nimble:ListStreamingImages",
"nimble:ListStreamingSessions",
"nimble:ListStudioComponents",
"nimble:ListStudioMembers",
"nimble:ListStudios",
"nimble:ListTagsForResource",
"notifications-contacts:GetEmailContact",
"notifications-contacts:ListEmailContacts",
"notifications-contacts:ListTagsForResource",
"notifications:GetEventRule",
"notifications:GetNotificationConfiguration",
"notifications:GetNotificationEvent",
"notifications:ListChannels",
"notifications:ListEventRules",
"notifications:ListNotificationConfigurations",
"notifications:ListNotificationEvents",
"notifications:ListNotificationHubs",
"notifications:ListTagsForResource",
"oam:GetLink",
"oam:GetSink",
"oam:GetSinkPolicy",
"oam:ListAttachedLinks",
"oam:ListLinks",
"oam:ListSinks",
"omics:Get*",
"omics:List*",
"one:GetDeviceConfigurationTemplate",
"one:GetDeviceInstance",
"one:GetDeviceInstanceConfiguration",
```

```
"one:GetSite",
"one:GetSiteAddress",
"one:ListDeviceConfigurationTemplates",
"one:ListDeviceInstances",
"one:ListSites",
"one:ListUsers",
"opsworks-cm:Describe*",
"opsworks-cm:List*",
"opsworks:Describe*",
"opsworks:Get*",
"organizations:Describe*",
"organizations:List*",
"osis:GetPipeline",
"osis:GetPipelineBlueprint",
"osis:GetPipelineChangeProgress",
"osis:ListPipelineBlueprints",
"osis:ListPipelines",
"osis:ListTagsForResource",
"outposts:Get*",
"outposts:List*",
"payment-cryptography:GetAlias",
"payment-cryptography:GetKey",
"payment-cryptography:GetPublicKeyCertificate",
"payment-cryptography:ListAliases",
"payment-cryptography:ListKeys",
"payment-cryptography:ListTagsForResource",
"payments:GetPaymentInstrument",
"payments:GetPaymentStatus",
"payments:ListPaymentPreferences",
"pca-connector-ad:GetConnector",
"pca-connector-ad:GetDirectoryRegistration",
"pca-connector-ad:GetServicePrincipalName",
"pca-connector-ad:GetTemplate",
"pca-connector-ad:GetTemplateGroupAccessControlEntry",
"pca-connector-ad:ListConnectors",
"pca-connector-ad:ListDirectoryRegistrations",
"pca-connector-ad:ListServicePrincipalNames",
"pca-connector-ad:ListTagsForResource",
"pca-connector-ad:ListTemplateGroupAccessControlEntries",
"pca-connector-ad:ListTemplates",
"personalize:Describe*",
"personalize:Get*",
"personalize:List*",
"pi:DescribeDimensionKeys",
```

```
"pi:GetDimensionKeyDetails",
"pi:GetResourceMetadata",
"pi:GetResourceMetrics",
"pi:ListAvailableResourceDimensions",
"pi:ListAvailableResourceMetrics",
"pipes:DescribePipe",
"pipes:ListPipes",
"pipes:ListTagsForResource",
"polly:Describe*",
"polly:Get*",
"polly:List*",
"polly:SynthesizeSpeech",
"pricing:DescribeServices",
"pricing:GetAttributeValues",
"pricing:GetPriceListFileUrl",
"pricing:GetProducts",
"pricing:ListPriceLists",
"proton:GetDeployment",
"proton:GetEnvironment",
"proton:GetEnvironmentTemplate",
"proton:GetEnvironmentTemplateVersion",
"proton:GetService",
"proton:GetServiceInstance",
"proton:GetServiceTemplate",
"proton:GetServiceTemplateVersion",
"proton:ListDeployments",
"proton:ListEnvironmentAccountConnections",
"proton:ListEnvironments",
"proton:ListEnvironmentTemplates",
"proton:ListServiceInstances",
"proton:ListServices",
"proton:ListServiceTemplates",
"proton:ListTagsForResource",
"purchase-orders:GetPurchaseOrder",
"purchase-orders:ListPurchaseOrderInvoices",
"purchase-orders:ListPurchaseOrders",
"purchase-orders:ViewPurchaseOrders",
"qldb:DescribeJournalKinesisStream",
"qldb:DescribeJournalS3Export",
"qldb:DescribeLedger",
"qldb:GetBlock",
"qldb:GetDigest",
"qldb:GetRevision",
"qldb:ListJournalKinesisStreamsForLedger",
```

```
"qldb:ListJournalS3Exports",
"qldb:ListJournalS3ExportsForLedger",
"qldb:ListLedgers",
"qldb:ListTagsForResource",
"ram:Get*",
"ram:List*",
"rbin:GetRule",
"rbin:ListRules",
"rbin:ListTagsForResource",
"rds:Describe*",
"rds:Download*",
"rds:List*",
"redshift:Describe*",
"redshift:GetReservedNodeExchangeOfferings",
"redshift:View*",
"refactor-spaces:GetApplication",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetResourcePolicy",
"refactor-spaces:GetRoute",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListEnvironmentVpcs",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
"refactor-spaces:ListTagsForResource",
"rekognition:CompareFaces",
"rekognition:DescribeDataset",
"rekognition:DescribeProjects",
"rekognition:DescribeProjectVersions",
"rekognition:DescribeStreamProcessor",
"rekognition:Detect*",
"rekognition:GetCelebrityInfo",
"rekognition:GetCelebrityRecognition",
"rekognition:GetContentModeration",
"rekognition:GetFaceDetection",
"rekognition:GetFaceSearch",
"rekognition:GetLabelDetection",
"rekognition:GetPersonTracking",
"rekognition:GetSegmentDetection",
"rekognition:GetTextDetection",
"rekognition:List*",
"rekognition:RecognizeCelebrities",
"rekognition:Search*",
```



```
"resiliencehub:DescribeApp",
"resiliencehub:DescribeAppAssessment",
"resiliencehub:DescribeAppVersion",
"resiliencehub:DescribeAppVersionAppComponent",
"resiliencehub:DescribeAppVersionResource",
"resiliencehub:DescribeAppVersionResourcesResolutionStatus",
"resiliencehub:DescribeAppVersionTemplate",
"resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
"resiliencehub:DescribeResiliencyPolicy",
"resiliencehub:ListAlarmRecommendations",
"resiliencehub:ListAppAssessmentComplianceDrifts",
"resiliencehub:ListAppAssessments",
"resiliencehub:ListAppComponentCompliances",
"resiliencehub:ListAppComponentRecommendations",
"resiliencehub:ListAppInputSources",
"resiliencehub:ListApps",
"resiliencehub:ListAppVersionAppComponents",
"resiliencehub:ListAppVersionResourceMappings",
"resiliencehub:ListAppVersionResources",
"resiliencehub:ListAppVersions",
"resiliencehub:ListRecommendationTemplates",
"resiliencehub:ListResiliencyPolicies",
"resiliencehub:ListSopRecommendations",
"resiliencehub:ListSuggestedResiliencyPolicies",
"resiliencehub:ListTagsForResource",
"resiliencehub:ListTestRecommendations",
"resiliencehub:ListUnsupportedAppVersionResources",
"resource-explorer-2:BatchGetView",
"resource-explorer-2:GetDefaultView",
"resource-explorer-2:GetIndex",
"resource-explorer-2:GetView",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListSupportedResourceTypes",
"resource-explorer-2:ListTagsForResource",
"resource-explorer-2:ListViews",
"resource-explorer-2:Search",
"resource-groups:Get*",
"resource-groups:List*",
"resource-groups:Search*",
"robomaker:BatchDescribe*",
"robomaker:Describe*",
"robomaker:Get*",
"robomaker:List*",
"route53-recovery-cluster:Get*",
```

```
"route53-recovery-cluster:ListRoutingControls",
"route53-recovery-control-config:Describe*",
"route53-recovery-control-config:GetResourcePolicy",
"route53-recovery-control-config:List*",
"route53-recovery-readiness:Get*",
"route53-recovery-readiness:List*",
"route53:Get*",
"route53:List*",
"route53:Test*",
"route53domains:Check*",
"route53domains:Get*",
"route53domains:List*",
"route53domains:View*",
"route53resolver:Get*",
"route53resolver:List*",
"rum:GetAppMonitor",
"rum:GetAppMonitorData",
"rum:ListAppMonitors",
"s3-object-lambda:GetObject",
"s3-object-lambda:GetObjectAcl",
"s3-object-lambda:GetObjectLegalHold",
"s3-object-lambda:GetObjectRetention",
"s3-object-lambda:GetObjectTagging",
"s3-object-lambda:GetObjectVersion",
"s3-object-lambda:GetObjectVersionAcl",
"s3-object-lambda:GetObjectVersionTagging",
"s3-object-lambda:ListBucket",
"s3-object-lambda:ListBucketMultipartUploads",
"s3-object-lambda:ListBucketVersions",
"s3-object-lambda:ListMultipartUploadParts",
"s3:DescribeJob",
"s3:Get*",
"s3:List*",
"sagemaker-groundtruth-synthetic:GetAccountDetails",
"sagemaker-groundtruth-synthetic:GetBatch",
"sagemaker-groundtruth-synthetic:GetProject",
"sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
"sagemaker-groundtruth-synthetic:ListBatchSummaries",
"sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
"sagemaker-groundtruth-synthetic:ListProjectSummaries",
"sagemaker:Describe*",
"sagemaker:GetSearchSuggestions",
"sagemaker:List*",
"sagemaker:Search",
```

```
"savingsplans:DescribeSavingsPlanRates",
"savingsplans:DescribeSavingsPlans",
"savingsplans:DescribeSavingsPlansOfferingRates",
"savingsplans:DescribeSavingsPlansOfferings",
"savingsplans:ListTagsForResource",
"scheduler:GetSchedule",
"scheduler:GetScheduleGroup",
"scheduler:ListScheduleGroups",
"scheduler:ListSchedules",
"scheduler:ListTagsForResource",
"schemas:Describe*",
"schemas:Get*",
"schemas:List*",
"schemas:Search*",
"sdb:Get*",
"sdb:List*",
"sdb:Select*",
"secretsmanager:Describe*",
"secretsmanager:GetResourcePolicy",
"secretsmanager:List*",
"securityhub:BatchGetControlEvaluations",
"securityhub:BatchGetSecurityControls",
"securityhub:BatchGetStandardsControlAssociations",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"serverlessrepo:Get*",
"serverlessrepo:List*",
"serverlessrepo:SearchApplications",
"servicecatalog:Describe*",
"servicecatalog:GetApplication",
"servicecatalog:GetAttributeGroup",
"servicecatalog:List*",
"servicecatalog:Scan*",
"servicecatalog:Search*",
"servicediscovery:DiscoverInstances",
"servicediscovery:DiscoverInstancesRevision",
"servicediscovery:Get*",
"servicediscovery:List*",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetRequestedServiceQuotaChange",
"servicequotas:GetServiceQuota",
"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
```

```
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"ses:BatchGetMetricData",
"ses:Describe*",
"ses:Get*",
"ses:List*",
"shield:Describe*",
"shield:Get*",
"shield:List*",
"signer:DescribeSigningJob",
"signer:GetSigningPlatform",
"signer:GetSigningProfile",
"signer:ListProfilePermissions",
"signer:ListSigningJobs",
"signer:ListSigningPlatforms",
"signer:ListSigningProfiles",
"signer:ListTagsForResource",
"sms-voice:DescribeAccountAttributes",
"sms-voice:DescribeAccountLimits",
"sms-voice:DescribeConfigurationSets",
"sms-voice:DescribeKeywords",
"sms-voice:DescribeOptedOutNumbers",
"sms-voice:DescribeOptOutLists",
"sms-voice:DescribePhoneNumbers",
"sms-voice:DescribePools",
"sms-voice: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" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

ResourceGroupsandTagEditorFullAccess

ResourceGroupsandTagEditorFullAccess es una [política administrada por AWS](#) que: concede acceso total a Resource Groups y Tag Editor.

Uso de la política

Puede asociar ResourceGroupsandTagEditorFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 10 de agosto de 2023 a las 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources",
        "resource-groups:*",
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ResourceGroupsandTagEditorReadOnlyAccess

ResourceGroupsandTagEditorReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso para utilizar Resource Groups y Tag Editor, pero no permite editar etiquetas con el Tag Editor.

Uso de la política

Puede asociar ResourceGroupsandTagEditorReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 10 de agosto de 2023 a las 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ResourceGroupsServiceRolePolicy

ResourceGroupsServiceRolePolicy es una [política administrada por AWS](#) que: permite que AWS Resource Groups consulte los servicios de AWS a los que pertenecen sus recursos para mantener el grupo actualizado

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de enero de 2023 a las 16:57 UTC
- Hora de edición: 5 de enero de 2023 a las 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
```

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

ROSAAmazonEBSCSIDriverOperatorPolicy es una [política administrada por AWS](#) que: permite al operador del controlador Amazon EBS Container Storage Interface (CSI) de OpenShift instalar y mantener el controlador CSI de Amazon EBS en un clúster de Red Hat OpenShift Service (ROSA) de AWS. El controlador de CSI de Amazon EBS permite que los clústeres de ROSA administren el ciclo de vida de los volúmenes de Amazon EBS para volúmenes persistentes.

Uso de la política

Puede asociar ROSAAmazonEBSCSIDriverOperatorPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 22:36 UTC
- Hora de edición: 20 de abril de 2023 a las 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2>DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
```

```
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "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"
      ]
    }
  }
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSACloudNetworkConfigOperatorPolicy

ROSACloudNetworkConfigOperatorPolicy es una [política administrada por AWS](#) que: permite al operador del controlador de configuración de red de OpenShift Cloud aprovisionar y gestionar los recursos de red para que el servicio Red Hat OpenShift on AWS (ROSA) los use para la superposición de red de clúster. El operador de red OpenShift Cloud interactúa con las API de AWS en nombre de los complementos de red mediante CustomResourceDefinitions. El operador utiliza estos permisos de política para administrar las direcciones IP privadas de las instancias de Amazon EC2 como parte del clúster ROSA.

Uso de la política

Puede asociar ROSACloudNetworkConfigOperatorPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 22:34 UTC
- Hora de edición: 20 de abril de 2023 a las 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAControlPlaneOperatorPolicy

R0SAControlPlane0peratorPolicy es una [política administrada por AWS](#) que: permite que el plano de control de Red Hat OpenShift Service on AWS (ROSA) gestione los recursos de Amazon EC2 y Amazon Route 53 del clúster ROSA.

Uso de la política

Puede asociar R0SAControlPlane0peratorPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de abril de 2023 a las 23:02 UTC
- Hora de edición: 30 de junio de 2023 a las 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "ReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeVpcs",
      "ec2:DescribeSecurityGroups",
      "route53:ListHostedZones"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CreateSecurityGroups",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group*/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "DeleteSecurityGroup",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group*/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  }
],
{
```

```

    "Sid" : "SecurityGroupIngressEgress",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "CreateSecurityGroupsVPCNoCondition",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*/*"
    ]
  },
  {
    "Sid" : "ListResourceRecordSets",
    "Effect" : "Allow",
    "Action" : [
      "route53:ListResourceRecordSets"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeResourceRecordSets"
    ],
    "Resource" : [

```

```
    "*"
  ],
  "Condition" : {
    "ForAllValues:StringLike" : {
      "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
        "*.hypershift.local"
      ]
    }
  }
},
{
  "Sid" : "VPCEndpointWithCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "VPCEndpointResourceTagCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "VPCEndpointNoCondition",
  "Effect" : "Allow",
  "Action" : [
```

```

    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "ManageVPCEndpointWithCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "ModifyVPCEndpoingNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "CreateTagsRestrictedActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},

```



```
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateVpcEndpoint",
          "CreateSecurityGroup"
        ]
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAImageRegistryOperatorPolicy

ROSAImageRegistryOperatorPolicy es una [política AWS administrada](#) que: permite al operador de registro de OpenShift imágenes aprovisionar y administrar buckets y objetos de Amazon S3 para que los utilice el OpenShift Servicio Red Hat en el registro de imágenes integrado en el clúster AWS (ROSA) a fin de cumplir con los requisitos de almacenamiento de ROSA. El operador OpenShift de registro de imágenes instala y mantiene el registro interno de un clúster de Red Hat. OpenShift

Uso de la política

Puede asociar ROSAImageRegistryOperatorPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de abril de 2023 a las 20:13 UTC

- Hora editada: 12 de diciembre de 2023 a las 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3>DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
    },
  ],
}
```

```

    "Resource" : [
      "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
      "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
    ]
  },
  {
    "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}/*"
    ]
  }
]
}

```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAIngressOperatorPolicy

ROSAIngressOperatorPolicy es una [política administrada por AWS](#) que: permite al operador de entrada de OpenShift aprovisionar y gestionar los balanceadores de carga y las configuraciones del sistema de nombres de dominio (DNS) para los clústeres de Red Hat OpenShift Service on AWS (ROSA). La política concede acceso de lectura a los valores de las etiquetas, que el operador filtra para que los recursos de Route 53 descubran las zonas alojadas.

Uso de la política

Puede asociar `ROSAIngressOperatorPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 22:37 UTC
- Hora de edición: 20 de abril de 2023 a las 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
"ForAllValues:StringLike" : {
  "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
    "*.openshiftapps.com",
    "*.devshift.org",
    "*.openshiftusgov.com",
    "*.devshiftusgov.com"
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAInstallerPolicy

ROSAInstallerPolicy es una [política AWS administrada](#) que: permite al instalador de Red Hat OpenShift Service on AWS (ROSA) administrar AWS los recursos que respaldan la instalación del clúster ROSA. Esto incluye la gestión de los perfiles de instancia para los nodos de trabajo de ROSA.

Uso de la política

Puede asociar ROSAInstallerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de junio de 2023 a las 21:00 UTC
- Hora editada: 26 de enero de 2024 a las 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Sid" : "PassRoleToEC2",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:*:iam:*:role/*-ROSA-Worker-Role"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ManageInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
    "iam:AddRoleToInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:instance-profile/rosa-service-managed-*"
  ]
},
{
  "Sid" : "CreateInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
    "iam>CreateInstanceProfile",
    "iam:TagInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:instance-profile/rosa-service-managed-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "GetSecretValue",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "Route53ManageRecords",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeResourceRecordSets"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringLike" : {
        "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
          "*.openshiftapps.com",
          "*.devshift.org",
          "*.hypershift.local",
          "*.openshiftusgov.com",
          "*.devshiftusgov.com"
        ]
      }
    }
  },
  {
    "Sid" : "Route53Manage",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeTagsForResource",
      "route53:CreateHostedZone",
      "route53>DeleteHostedZone"
    ],
```



```
    "Resource" : "*"
  },
  {
    "Sid" : "CreateTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "RunInstances"
        ]
      }
    }
  },
  {
    "Sid" : "RunInstancesNoCondition",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:snapshot*"
    ]
  },
  {
    "Sid" : "RunInstancesRestrictedRequestTag",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  }
}
```

```
},
{
  "Sid" : "RunInstancesRedHatOwnedAMIs",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:image/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:Owner" : [
        "531415883065",
        "251351625822",
        "210686502322"
      ]
    }
  }
},
{
  "Sid" : "ManageInstancesRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances",
    "ec2:GetConsoleOutput"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateGrantRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
}
```

```
    },
    "StringLike" : {
      "kms:ViaService" : "ec2.*.amazonaws.com"
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    }
  }
},
{
  "Sid" : "ManagedKMSRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "DeleteSecurityGroup",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSecurityGroup"
  ],
}
```

```

    "Resource" : [
      "arn:aws:ec2:*:*:security-group*/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "SecurityGroupIngressEgress",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group*/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "CreateSecurityGroupsVPCNoCondition",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*"
    ]
  },
  {
    "Sid" : "CreateTagsRestrictedActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [

```

```
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateSecurityGroup"
      ]
    }
  }
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAKMSProviderPolicy

ROSAKMSProviderPolicy es una [política administrada por AWS](#) que: permite al proveedor de cifrado ROSA integrado de AWS gestionar las claves AWS Key Management Service (KMS) para respaldar el cifrado de datos etcd utilizando una clave AWS KMS proporcionada por el cliente. La política permite cifrar y descifrar los datos con las claves KMS.

Uso de la política

Puede asociar ROSAKMSProviderPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de abril de 2023 a las 20:10 UTC
- Hora de edición: 27 de abril de 2023 a las 20:10 UTC

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

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAKubeControllerPolicy

ROSAKubeControllerPolicy es una [política administrada por AWS](#) que: permite que el controlador de Kubernetes ROSA gestione los recursos de Amazon EC2, Elastic Load Balancing (ELB) y AWS Key Management Service (KMS) para un clúster de ROSA.

Uso de la política

Puede asociar ROSAKubeControllerPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de abril de 2023 a las 20:09 UTC
- Hora de edición: 16 de octubre de 2023 a las 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
```

```

    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeLoadBalancerPolicies"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "KMSDescribeKey",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
},
{
  "Sid" : "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"
    }
  }
}
]
```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAManageSubscription

ROSAManageSubscription es una [política administrada por AWS](#) que: concede los permisos necesarios para administrar la suscripción a Red Hat OpenShift Service on AWS (ROSA).

Uso de la política

Puede asociar ROSAManageSubscription a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 11 de abril de 2022 a las 20:58 UTC
- Hora de edición: 4 de agosto de 2023 a las 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSANodePoolManagementPolicy

ROSANodePoolManagementPolicy es una [política administrada por AWS](#) que: permite que Red Hat OpenShift Service on AWS (ROSA) gestione las instancias EC2 del clúster como nodos de trabajo, incluido el permiso para configurar grupos de seguridad y etiquetar instancias y volúmenes. Esta política también permite el uso de instancias EC2 con cifrado de disco proporcionado por las claves de AWS Key Management Service (KMS).

Uso de la política

Puede asociar ROSANodePoolManagementPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 8 de junio de 2023 a las 20:48 UTC
- Hora de edición: 8 de junio de 2023 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSASRESupportPolicy

ROSASRESupportPolicy es una [política AWS administrada](#) que: proporciona a la ingeniería de confiabilidad del sitio (SRE) de ROSA los permisos necesarios para observar, diagnosticar y respaldar inicialmente AWS los recursos asociados con el OpenShift Servicio Red Hat en los clústeres AWS (ROSA), incluida la capacidad de cambiar el estado de los nodos del clúster ROSA.

Uso de la política

Puede asociar ROSASRESupportPolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de junio de 2023 a las 14:36 UTC
- Hora de edición: 22 de enero de 2024 a las 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "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"
    }
}
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ROSAWorkerInstancePolicy

ROSAWorkerInstancePolicy es una [política administrada AWS](#) que: permite que los nodos de trabajo de Red Hat OpenShift Service on AWS (ROSA) de su cuenta tengan acceso de solo lectura a las instancias de Amazon EC2 y las Regiones de AWS, para administrar el ciclo de vida de los nodos de cómputo.

Uso de la política

Puede asociar ROSAWorkerInstancePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 22:35 UTC
- Hora de edición: 20 de abril de 2023 a las 22:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

Route53RecoveryReadinessServiceRolePolicy

Route53RecoveryReadinessServiceRolePolicy es una [política administrada por AWS](#) que: Política de roles vinculados a un servicio para Route 53 Recovery Readiness

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 15 de julio de 2021 a las 16:06 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/AWSServiceRoleForServiceQuotas",
    }
  ]
}
```

```
"Condition" : {
  "StringLike" : {
    "iam:AWSServiceName" : "servicequotas.amazonaws.com"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetFunctionConcurrency",
    "lambda:GetFunctionConfiguration",
    "lambda:GetProvisionedConcurrencyConfig",
    "lambda:ListProvisionedConcurrencyConfigs",
    "lambda:ListAliases",
    "lambda:ListVersionsByFunction"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBClusters"
  ],
  "Resource" : "arn:aws:rds:*:*:cluster:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBInstances"
  ],
  "Resource" : "arn:aws:rds:*:*:db:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53:ListResourceRecordSets"
  ],
  "Resource" : "arn:aws:route53:::hostedzone/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53:GetHealthCheck",
    "route53:GetHealthCheckStatus"
  ]
}
```

```
    ],
    "Resource" : "arn:aws:route53:::healthcheck/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:RequestServiceQuotaIncrease"
    ],
    "Resource" : "arn:aws:servicequotas:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:GetTopicAttributes",
      "sns:ListSubscriptionsByTopic"
    ],
    "Resource" : "arn:aws:sns:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:GetQueueAttributes",
      "sqs:GetQueueUrl"
    ],
    "Resource" : "arn:aws:sqs:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingPolicies",
      "autoscaling:DescribeAccountLimits",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribeAutoScalingInstances",
      "autoscaling:DescribeLifecycleHooks",
      "autoscaling:DescribeLoadBalancers",
      "autoscaling:DescribeLoadBalancerTargetGroups",
      "autoscaling:DescribeNotificationConfigurations",
      "autoscaling:DescribePolicies",
      "cloudwatch:GetMetricData",
      "cloudwatch:DescribeAlarms",
      "dynamodb:DescribeLimits",
      "dynamodb:ListGlobalTables",
```

```

    "dynamodb:ListTables",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:GetEbsDefaultKmsKeyId",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "kafka:DescribeCluster",
    "kafka:DescribeConfigurationRevision",
    "lambda:ListEventSourceMappings",
    "lambda:ListFunctions",
    "rds:DescribeAccountAttributes",
    "route53:GetHostedZone",
    "servicequotas:ListAWSDefaultServiceQuotas",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas",
    "servicequotas:ListServices",
    "sns:GetEndpointAttributes",
    "sns:GetSubscriptionAttributes"
  ],
  "Resource" : "*"
}
]
}

```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

Route53ResolverServiceRolePolicy

Route53ResolverServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y los recursos utilizados o administrados por Route53 Resolver

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de agosto de 2020 a las 17:47 UTC
- Hora de edición: 12 de agosto de 2020 a las 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
```



```
    "logs:DescribeResourcePolicies",
    "logs:DescribeLogGroups",
    "s3:GetBucketPolicy"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

S3StorageLensServiceRolePolicy

S3StorageLensServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y a los recursos utilizados o gestionados por S3 Storage Lens

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2020 a las 18:15 UTC
- Hora de edición: 18 de noviembre de 2020 a las 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

SecretsManagerReadWrite

SecretsManagerReadWrite es una [política AWS gestionada](#) que: proporciona acceso de lectura y escritura a AWS Secrets Manager a través de. AWS Management Console Nota: esto excluye las acciones de IAM, así que combínelas con las de IAM si se requiere una configuración de rotación.

FullAccess

Uso de la política

Puede asociar `SecretsManagerReadWrite` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 4 de abril de 2018 a las 18:05 UTC
- Hora editada: 22 de febrero de 2024 a las 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
```

```

    "kms:ListAliases",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstances",
    "redshift:DescribeClusters",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LambdaPermissions",
  "Effect" : "Allow",
  "Action" : [
    "lambda:AddPermission",
    "lambda:CreateFunction",
    "lambda:GetFunction",
    "lambda:InvokeFunction",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
},
{
  "Sid" : "SARPermissions",
  "Effect" : "Allow",
  "Action" : [
    "serverlessrepo:CreateCloudFormationChangeSet",
    "serverlessrepo:GetApplication"
  ],
  "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
},
{
  "Sid" : "S3Permissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::awsserverlessrepo-changesets*",
    "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
  ]
}

```

```
]
}
```

Más información

- [Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

SecurityAudit

SecurityAudit es una [política administrada por AWS](#) en la que: la plantilla de auditoría de seguridad otorga acceso para leer los metadatos de la configuración de seguridad. Sirve para el software que audita la configuración de una Cuenta de AWS.

Uso de la política

Puede asociar SecurityAudit a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora editada: 14 de diciembre de 2023, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Versión de la política

Versión de la política: v41 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "BaseSecurityAuditStatement",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
```

```
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appsync:GetApiCache",
"appsync:List*",
"athena:GetWorkGroup",
"athena:List*",
"auditmanager:GetAccountStatus",
"auditmanager:ListAssessmentControlInsightsByControlDomain",
"auditmanager:ListAssessmentFrameworks",
"auditmanager:ListAssessmentFrameworkShareRequests",
"auditmanager:ListAssessmentReports",
"auditmanager:ListAssessments",
"auditmanager:ListControlDomainInsights",
"auditmanager:ListControlDomainInsightsByAssessment",
"auditmanager:ListControlInsightsByControlDomain",
"auditmanager:ListControls",
"auditmanager:ListNotifications",
"auditmanager:ListTagsForResource",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling:Describe*",
"backup:DescribeRegionSettings",
"backup:GetBackupVaultAccessPolicy",
"backup:ListBackupVaults",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobDefinitions",
"braket:SearchJobs",
"braket:SearchQuantumTasks",
"chime:List*",
"cloud9:Describe*",
"cloud9:ListEnvironments",
"clouddirectory:ListDirectories",
"cloudformation:DescribeStack*",
"cloudformation:GetStackPolicy",
"cloudformation:GetTemplate",
"cloudformation:ListStack*",
"cloudfront:Get*",
"cloudfront:List*",
"cloudsearch:DescribeDomainEndpointOptions",
"cloudsearch:DescribeDomains",
```

```
"cloudsearch:DescribeServiceAccessPolicies",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrail",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"cloudtrail:LookupEvents",
"cloudwatch:Describe*",
"cloudwatch:GetDashboard",
"cloudwatch:ListTagsForResource",
"cloudwatch:ListDashboards",
"codeartifact:GetDomainPermissionsPolicy",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListRepositories",
"codebuild:BatchGetProjects",
"codebuild:ListProjects",
"codecommit:BatchGetRepositories",
"codecommit:GetBranch",
"codecommit:GetObjectIdentifier",
"codecommit:GetRepository",
"codecommit:GetRepositoryTriggers",
"codecommit:List*",
"codedeploy:Batch*",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:GetJobDetails",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineExecution",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"codestar:Describe*",
"codestar:List*",
"cognito-identity:Describe*",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:ListIdentityPools",
"cognito-identity:ListTagsForResource",
"cognito-idp:Describe*",
"cognito-idp:ListDevices",
"cognito-idp:ListGroups",
"cognito-idp:ListIdentityProviders",
"cognito-idp:ListResourceServers",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserImportJobs",
"cognito-idp:ListUserPoolClients",
```



```
"cognito-idp:ListUserPools",
"cognito-idp:ListUsers",
"cognito-idp:ListUsersInGroup",
"cognito-sync:Describe*",
"cognito-sync:List*",
"comprehend:Describe*",
"comprehend:List*",
"comprehendmedical:ListICD10CMInferenceJobs",
"comprehendmedical:ListPHIDetectionJobs",
"comprehendmedical:ListRxNormInferenceJobs",
"comprehendmedical:ListSNOMEDCTInferenceJobs",
"config:BatchGetAggregateResourceConfig",
"config:BatchGetResourceConfig",
"config:Deliver*",
"config:Describe*",
"config:Get*",
"config:List*",
"config>SelectAggregateResourceConfig",
"config>SelectResourceConfig",
"connect:ListInstances",
"dataexchange:ListDataSets",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:EvaluateExpression",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:QueryObjects",
"datapipeline:ValidatePipelineDefinition",
"datasync:Describe*",
"datasync:List*",
"dax:Describe*",
"dax:ListTags",
"deepracer:ListModels",
"detective:GetGraphIngestState",
"detective:ListGraphs",
"detective:ListMembers",
"devicefarm:ListProjects",
"directconnect:Describe*",
"discovery:DescribeAgents",
"discovery:DescribeConfigurations",
"discovery:DescribeContinuousExports",
"discovery:DescribeExportConfigurations",
"discovery:DescribeExportTasks",
"discovery:DescribeImportTasks",
```

```
"dms:Describe*",
"dms:ListTagsForResource",
"docdb-elastic:ListClusters",
"ds:DescribeDirectories",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetImageBlockPublicAccessState",
"ec2:GetManagedPrefixListAssociations",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ec2:GetTransitGatewayAttachmentPropagations",
"ec2:GetTransitGatewayMulticastDomainAssociations",
"ec2:GetTransitGatewayPrefixListReferences",
"ec2:GetTransitGatewayRouteTableAssociations",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:SearchTransitGatewayRoutes",
"ecr-public:DescribeImages",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribeImages",
"ecr:DescribeImageScanFindings",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRegistryPolicy",
"ecr:GetRegistryScanningConfiguration",
"ecr:GetRepositoryPolicy",
"ecr:ListImages",
```

```
"ecr:ListTagsForResource",
"ecs:Describe*",
"ecs:List*",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodeGroup",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListNodeGroups",
"eks:ListUpdates",
"elastic-inference:DescribeAccelerators",
"elasticache:Describe*",
"elasticache:ListTagsForResource",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:ListTagsForResource",
"elasticfilesystem:DescribeAccountPreferences",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticfilesystem:DescribeTags",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elastictranscoder:ListPipelines",
"es:Describe*",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListElasticsearchInstanceTypeDetails",
"es:ListElasticsearchVersions",
"es:ListTags",
"events:Describe*",
"events:List*",
"events:TestEventPattern",
"finspace:ListEnvironments",
"finspace:ListKxEnvironments",
"firehose:Describe*",
"firehose:List*",
```

```
"fms:ListComplianceStatus",
"fms:ListPolicies",
"forecast:ListDatasets",
"frauddetector:GetDetectors",
"fsx:Describe*",
"fsx:List*",
"gamelift:ListBuilds",
"gamelift:ListFleets",
"geo:ListMaps",
"glacier:DescribeVault",
"glacier:GetVaultAccessPolicy",
"glacier:GetVaultLock",
"glacier:ListVaults",
"globalaccelerator:Describe*",
"globalaccelerator:List*",
"glue:GetCrawlers",
"glue:GetDatabases",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDevEndpoints",
"glue:GetJobs",
"glue:GetResourcePolicy",
"glue:GetSecurityConfigurations",
"grafana:ListWorkspaces",
"greengrass:List*",
"guardduty:DescribePublishingDestination",
"guardduty:Get*",
"guardduty:List*",
"health:DescribeAffectedEntities",
"health:DescribeEntityAggregates",
"health:DescribeEventAggregates",
"health:DescribeEvents",
"health:DescribeEventTypes",
"healthlake:ListFHIRDatastores",
"honeycode:ListTables",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"iam:SimulateCustomPolicy",
"iam:SimulatePrincipalPolicy",
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
```

```
"inspector2:BatchGetAccountStatus",
"inspector2:BatchGetFreeTrialInfo",
"inspector2:DescribeOrganizationConfiguration",
"inspector2:GetConfiguration",
"inspector2:GetDelegatedAdminAccount",
"inspector2:GetFindingsReportStatus",
"inspector2:GetMember",
"inspector2:ListAccountPermissions",
"inspector2:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"iot:Describe*",
"iot:GetPolicy",
"iot:GetPolicyVersion",
"iot:List*",
"iotanalytics:ListChannels",
"iotevents:ListInputs",
"iotfleetwise:ListModelManifests",
"iotsitewise:DescribeGatewayCapabilityConfiguration",
"iotsitewise:ListAssetModels",
"iotsitewise:ListGateways",
"iottwinmaker:ListWorkspaces",
"kafka-cluster:Describe*",
"kafka:Describe*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafkaconnect:Describe*",
"kafkaconnect:List*",
"kendra:DescribeIndex",
"kendra:ListIndices",
"kinesis:DescribeLimits",
"kinesis:DescribeStream",
"kinesis:DescribeStreamConsumer",
"kinesis:DescribeStreamSummary",
"kinesis:ListShards",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
```

```
"kinesisanalytics:ListApplications",
"kinesisvideo:DescribeEdgeConfiguration",
"kinesisvideo:DescribeMappedResourceConfiguration",
"kinesisvideo:DescribeMediaStorageConfiguration",
"kinesisvideo:DescribeNotificationConfiguration",
"kinesisvideo:DescribeSignalingChannel",
"kinesisvideo:DescribeStream",
"kinesisvideo:ListSignalingChannels",
"kinesisvideo:ListStreams",
"kinesisvideo:ListTagsForResource",
"kinesisvideo:ListTagsForStream",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lambda:GetAccountSettings",
"lambda:GetFunctionConfiguration",
"lambda:GetFunctionEventInvokeConfig",
"lambda:GetLayerVersionPolicy",
"lambda:GetPolicy",
"lambda:List*",
"lex:DescribeBot",
"lex:DescribeResourcePolicy",
"lex:ListBots",
"license-manager:List*",
"lightsail:GetDisks",
"lightsail:GetDiskSnapshots",
"lightsail:GetInstances",
"lightsail:GetLoadBalancers",
"logs:Describe*",
"logs:ListTagsLogGroup",
"lookoutequipment:ListDatasets",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutvision:ListProjects",
"machinelearning:DescribeMLModels",
"managedblockchain:ListNetworks",
"mechanicalturk:ListHITS",
"mediaconnect:Describe*",
"mediaconnect:List*",
"medialive:ListChannels",
"mediapackage-vod:DescribePackagingGroup",
"mediapackage-vod:ListPackagingGroups",
"mediapackage:DescribeOriginEndpoint",
"mediapackage:ListOriginEndpoints",
"mediastore:GetContainerPolicy",
```

```
"mediastore:GetCorsPolicy",
"mediastore:ListContainers",
"memorydb:DescribeClusters",
"mq:DescribeBroker",
"mq:DescribeBrokerEngineTypes",
"mq:DescribeBrokerInstanceOptions",
"mq:DescribeConfiguration",
"mq:DescribeConfigurationRevision",
"mq:DescribeUser",
"mq:ListBrokers",
"mq:ListConfigurationRevisions",
"mq:ListConfigurations",
"mq:ListTags",
"mq:ListUsers",
"network-firewall:DescribeFirewall",
"network-firewall:DescribeFirewallPolicy",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:DescribeResourcePolicy",
"network-firewall:DescribeRuleGroup",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"network-firewall:ListRuleGroups",
"networkmanager:DescribeGlobalNetworks",
"nimble:ListStudios",
"opsworks-cm:DescribeServers",
"opsworks:DescribeStacks",
"organizations:Describe*",
"organizations:List*",
"personalize:DescribeDatasetGroup",
"personalize:ListDatasetGroups",
"private-networks:ListNetworks",
"qldb:DescribeJournalS3Export",
"qldb:DescribeLedger",
"qldb:ListJournalS3Exports",
"qldb:ListJournalS3ExportsForLedger",
"qldb:ListLedgers",
"quicksight:Describe*",
"quicksight:List*",
"ram:GetResourceShares",
"ram:List*",
"rds:Describe*",
"rds:DownloadDBLogFilePortion",
"rds:ListTagsForResource",
"redshift:Describe*",
```

```
"rekognition:Describe*",
"rekognition:List*",
"resource-groups:ListGroupResources",
"robomaker:Describe*",
"robomaker:List*",
"route53:Get*",
"route53:List*",
"route53domains:GetDomainDetail",
"route53domains:GetOperationDetail",
"route53domains:ListDomains",
"route53domains:ListOperations",
"route53domains:ListTagsForDomain",
"route53resolver:Get*",
"route53resolver:List*",
"s3-outposts:ListEndpoints",
"s3-outposts:ListOutpostsWithS3",
"s3-outposts:ListSharedEndpoints",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetAnalyticsConfiguration",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetInventoryConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMetricsConfiguration",
"s3:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"sagemaker:Describe*",
"sagemaker:List*",
"schemas:DescribeCodeBinding",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemas",
"schemas:ListSchemaVersions",
```



```
"schemas:ListTagsForResource",
"sdb:DomainMetadata",
"sdb:ListDomains",
"secretsmanager:DescribeSecret",
"secretsmanager:GetResourcePolicy",
"secretsmanager:ListSecrets",
"secretsmanager:ListSecretVersionIds",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"serverlessrepo:GetApplicationPolicy",
"serverlessrepo:List*",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetRequestedServiceQuotaChange",
"servicequotas:GetServiceQuota",
"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"servicequotas:ListTagsForResource",
"ses:Describe*",
"ses:GetAccountSendingEnabled",
"ses:GetIdentityDkimAttributes",
"ses:GetIdentityPolicies",
"ses:GetIdentityVerificationAttributes",
"ses:ListConfigurationSets",
"ses:ListIdentities",
"ses:ListIdentityPolicies",
"ses:ListReceiptRuleSets",
"ses:ListVerifiedEmailAddresses",
"shield:Describe*",
"shield:GetSubscriptionState",
"shield:List*",
"snowball:ListClusters",
"snowball:ListJobs",
"sns:GetPlatformApplicationAttributes",
"sns:GetTopicAttributes",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTagsForResource",
```

```
"sns:ListTopics",
"sqs:GetQueueAttributes",
"sqs:ListDeadLetterSourceQueues",
"sqs:ListQueues",
"sqs:ListQueueTags",
"ssm:Describe*",
"ssm:GetAutomationExecution",
"ssm:ListAssociations",
"ssm:ListAssociationVersions",
"ssm:ListCommands",
"ssm:ListComplianceItems",
"ssm:ListComplianceSummaries",
"ssm:ListDocumentMetadataHistory",
"ssm:ListDocuments",
"ssm:ListDocumentVersions",
"ssm:ListInventoryEntries",
"ssm:ListOpsMetadata",
"ssm:ListResourceComplianceSummaries",
"ssm:ListResourceDataSync",
"ssm:ListTagsForResource",
"sso:DescribeAccountAssignmentCreationStatus",
"sso:DescribePermissionSet",
"sso:DescribePermissionsPolicies",
"sso:List*",
"states:DescribeStateMachine",
"states:ListStateMachines",
"storagegateway:DescribeBandwidthRateLimit",
"storagegateway:DescribeCache",
"storagegateway:DescribeCachediSCSIVolumes",
"storagegateway:DescribeGatewayInformation",
"storagegateway:DescribeMaintenanceStartTime",
"storagegateway:DescribeNFSFileShares",
"storagegateway:DescribeSnapshotSchedule",
"storagegateway:DescribeStorediSCSIVolumes",
"storagegateway:DescribeTapeArchives",
"storagegateway:DescribeTapeRecoveryPoints",
"storagegateway:DescribeTapes",
"storagegateway:DescribeUploadBuffer",
"storagegateway:DescribeVTLDevices",
"storagegateway:DescribeWorkingStorage",
"storagegateway:List*",
"sts:GetAccessKeyInfo",
"support:DescribeTrustedAdvisorCheckRefreshStatuses",
"support:DescribeTrustedAdvisorCheckResult",
```

```
"support:DescribeTrustedAdvisorChecks",
"support:DescribeTrustedAdvisorCheckSummaries",
"synthetics:DescribeCanaries",
"synthetics:DescribeCanariesLastRun",
"synthetics:DescribeRuntimeVersions",
"synthetics:GetCanary",
"synthetics:GetCanaryRuns",
"synthetics:GetGroup",
"synthetics>ListAssociatedGroups",
"synthetics>ListGroupResources",
"synthetics>ListGroups",
"synthetics>ListTagsForResource",
"tag:GetResources",
"tag:GetTagKeys",
"transcribe:GetCallAnalyticsCategory",
"transcribe:GetMedicalVocabulary",
"transcribe:GetVocabulary",
"transcribe:GetVocabularyFilter",
"transcribe>ListCallAnalyticsCategories",
"transcribe>ListCallAnalyticsJobs",
"transcribe>ListLanguageModels",
"transcribe>ListMedicalTranscriptionJobs",
"transcribe>ListMedicalVocabularies",
"transcribe>ListTagsForResource",
"transcribe>ListTranscriptionJobs",
"transcribe>ListVocabularies",
"transcribe>ListVocabularyFilters",
"transfer:Describe*",
"transfer>List*",
"translate>List*",
"trustedadvisor:Describe*",
"waf-regional:GetWebACL",
"waf-regional>ListResourcesForWebACL",
"waf-regional>ListTagsForResource",
"waf-regional>ListWebACLs",
"waf:GetWebACL",
"waf>ListTagsForResource",
"waf>ListWebACLs",
"wafv2:GetWebACL",
"wafv2:GetWebACLForResource",
"wafv2>ListAvailableManagedRuleGroups",
"wafv2>ListIPSets",
"wafv2>ListLoggingConfigurations",
"wafv2>ListRegexPatternSets",
```

```

    "wafv2:ListResourcesForWebACL",
    "wafv2:ListRuleGroups",
    "wafv2:ListTagsForResource",
    "wafv2:ListWebACLs",
    "workdocs:DescribeResourcePermissions",
    "workspaces:Describe*",
    "xray:GetEncryptionConfig",
    "xray:GetGroup",
    "xray:GetGroups",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetTraceSummaries",
    "xray:ListTagsForResource"
  ]
},
{
  "Effect" : "Allow",
  "Sid" : "APIGatewayAccess",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/apis",
    "arn:aws:apigateway:*::/apis/*/authorizers/*",
    "arn:aws:apigateway:*::/apis/*/authorizers",
    "arn:aws:apigateway:*::/apis/*/cors",
    "arn:aws:apigateway:*::/apis/*/deployments/*",
    "arn:aws:apigateway:*::/apis/*/deployments",
    "arn:aws:apigateway:*::/apis/*/exports/*",
    "arn:aws:apigateway:*::/apis/*/integrations/*",
    "arn:aws:apigateway:*::/apis/*/integrations",
    "arn:aws:apigateway:*::/apis/*/models/*",
    "arn:aws:apigateway:*::/apis/*/models",
    "arn:aws:apigateway:*::/apis/*/routes/*",
    "arn:aws:apigateway:*::/apis/*/routes",
    "arn:aws:apigateway:*::/apis/*/stages",
    "arn:aws:apigateway:*::/apis/*/stages/*",
    "arn:aws:apigateway:*::/clientcertificates",
    "arn:aws:apigateway:*::/clientcertificates/*",
    "arn:aws:apigateway:*::/domainnames",
    "arn:aws:apigateway:*::/domainnames/*/apimappings",
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/authorizers/*",
    "arn:aws:apigateway:*::/restapis/*/authorizers",

```

```

    "arn:aws:apigateway:*::/restapis/*/deployments/*",
    "arn:aws:apigateway:*::/restapis/*/deployments",
    "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
    "arn:aws:apigateway:*::/restapis/*/documentation/parts",
    "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
    "arn:aws:apigateway:*::/restapis/*/documentation/versions",
    "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
    "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
    "arn:aws:apigateway:*::/restapis/*/models/*",
    "arn:aws:apigateway:*::/restapis/*/models",
    "arn:aws:apigateway:*::/restapis/*/requestvalidators",
    "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*",
    "arn:aws:apigateway:*::/restapis/*/resources",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/tags/*",
    "arn:aws:apigateway:*::/vpclinks"
  ]
}
]
}
```

Más información

- [Cree un conjunto de permisos utilizando las políticas administradas de AWS en el IAM Identity Center](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

SecurityLakeServiceLinkedRole

SecurityLakeServiceLinkedRole es una [política administrada por AWS](#) que: concede permisos para operar el servicio Amazon Security Lake en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2022 a las 14:03 UTC
- Hora editada: 29 de febrero de 2024 a las 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```

    "Action" : [
      "organizations:DescribeAccount"
    ],
    "Resource" : [
      "arn:aws:organizations::*:account/o-*/*"
    ]
  },
  {
    "Sid" : "AllowManagementOfServiceLinkedChannel",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:CreateServiceLinkedChannel",
      "cloudtrail>DeleteServiceLinkedChannel",
      "cloudtrail:GetServiceLinkedChannel",
      "cloudtrail:UpdateServiceLinkedChannel"
    ],
    "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
  },
  {
    "Sid" : "AllowListServiceLinkedChannel",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:ListServiceLinkedChannels"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DescribeAnyVpc",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ListDelegatedAdmins",
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
      }
    }
  }
}

```

```
    }
  },
  {
    "Sid" : "AllowWafLoggingConfiguration",
    "Effect" : "Allow",
    "Action" : [
      "wafv2:PutLoggingConfiguration",
      "wafv2:GetLoggingConfiguration",
      "wafv2:ListLoggingConfigurations",
      "wafv2>DeleteLoggingConfiguration"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "wafv2:LogScope" : "SecurityLake"
      }
    }
  },
  {
    "Sid" : "AllowPutLoggingConfiguration",
    "Effect" : "Allow",
    "Action" : [
      "wafv2:PutLoggingConfiguration"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
      }
    }
  },
  {
    "Sid" : "ListWebACLs",
    "Effect" : "Allow",
    "Action" : [
      "wafv2:ListWebACLs"
    ],
    "Resource" : "*"
  }
]
```


Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos](#)

ServerMigration_ServiceRole

ServerMigration_ServiceRole es una [política administrada por AWS](#) que: otorga los permisos para que el AWS Server Migration Service migre las MV a EC2. Esto permite que el Server Migration Service coloque los recursos migrados en la cuenta de EC2 del cliente.

Uso de la política

Puede asociar ServerMigration_ServiceRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de agosto de 2020 a las 20:41 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

    "Action" : [
      "cloudformation:CreateChangeSet",
      "cloudformation:CreateStack"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**",
    "Condition" : {
      "Null" : {
        "cloudformation:ResourceTypes" : "false"
      },
      "ForAllValues:StringEquals" : {
        "cloudformation:ResourceTypes" : [
          "AWS::EC2::Instance",
          "AWS::ApplicationInsights::Application",
          "AWS::ResourceGroups::Group"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation>DeleteStack",
      "cloudformation:ExecuteChangeSet",
      "cloudformation>DeleteChangeSet",
      "cloudformation:DescribeChangeSet",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResource",
      "cloudformation:DescribeStackResources",
      "cloudformation:GetTemplate"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ValidateTemplate",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [

```

```

    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3>DeleteObject",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::sms-app-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sms:CreateReplicationJob",
    "sms>DeleteReplicationJob",
    "sms:GetReplicationJobs",
    "sms:GetReplicationRuns",
    "sms:GetServers",
    "sms:ImportServerCatalog",
    "sms:StartOnDemandReplicationRun",
    "sms:UpdateReplicationJob"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ssm:*::document/AWS-RunRemoteScript",
    "arn:aws:s3:::sms-app-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ssm:resourceTag/UseForSMSApplicationValidation" : [
        "true"
      ]
    }
  ]
}

```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:CancelCommand",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CopySnapshot"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CopySnapshot",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/SMSJobId" : [
        "sms-*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifySnapshotAttribute",
    "ec2>DeleteSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/SMSJobId" : [
        "sms-*"
      ]
    }
  }
}
```

```

    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSnapshotAttribute",
    "ec2:DeregisterImage",
    "ec2:ImportImage",
    "ec2:DescribeImportImageTasks",
    "ec2:GetEbsEncryptionByDefault"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:GetInstanceProfile"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    }
  }
},
{
  "Effect" : "Allow",

```

```
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : "cloudformation.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ServerMigrationConnector

ServerMigrationConnector es una [política administrada por AWS](#) que: permite que el AWS Server Migration Connector migre las MV a EC2. Permite la comunicación con el Servicio de migración de servidores de AWS, el acceso de lectura y escritura a los depósitos de S3 que comiencen por “sms-b-” y “import-to-ec2-”, así como a los depósitos que se utilizan para actualizar

AWS Server Migration Connector, el registro del AWS Server Migration Connector en AWS, y la carga las métricas en AWS.

Uso de la política

Puede asociar `ServerMigrationConnector` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de octubre de 2016 a las 21:45 UTC
- Hora de edición: 24 de octubre de 2016 a las 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
      "Resource" : "*"
    }
  ],
}
```

```

{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3>DeleteObject",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutLifecycleConfiguration",
    "s3:AbortMultipartUpload",
    "s3:ListBucketMultipartUploads",
    "s3:ListMultipartUploadParts"
  ],
  "Resource" : [
    "arn:aws:s3:::sms-b-*",
    "arn:aws:s3:::import-to-ec2-*",
    "arn:aws:s3:::server-migration-service-upgrade",
    "arn:aws:s3:::server-migration-service-upgrade/*",
    "arn:aws:s3:::connector-platform-upgrade-info/*",
    "arn:aws:s3:::connector-platform-upgrade-info",
    "arn:aws:s3:::connector-platform-upgrade-bundles/*",
    "arn:aws:s3:::connector-platform-upgrade-bundles",
    "arn:aws:s3:::connector-platform-release-notes/*",
    "arn:aws:s3:::connector-platform-release-notes"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "awsconnector:*",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "SNS:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
}
]
}

```


Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ServerMigrationServiceConsoleFullAccess

ServerMigrationServiceConsoleFullAccess es una [política administrada por AWS](#) que concede los permisos necesarios para usar todas las características de la consola del Server Migration Connector

Uso de la política

Puede asociar ServerMigrationServiceConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 9 de mayo de 2020 a las 17:18 UTC
- Hora de edición: 20 de julio de 2020 a las 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "sms:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "cloudformation:ListStacks",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackResources"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : "s3:ListAllMyBuckets",
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "arn:aws:s3:::sms-app-*/*"
  },
  {
    "Action" : [
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iam:ListRoles"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

```
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sms.amazonaws.com"
        }
      },
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ServerMigrationServiceLaunchRole

ServerMigrationServiceLaunchRole es una [política administrada por AWS](#) que: permite que el Server Migration Service de AWS cree y actualice los recursos pertinentes de AWS en la Cuenta de AWS del cliente para lanzar las aplicaciones y los servidores migrados.

Uso de la política

Puede asociar ServerMigrationServiceLaunchRole a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de noviembre de 2018 a las 19:53 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
            "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```

    "Resource" : "arn:aws:ec2:*:*:instance/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DisassociateIamInstanceProfile",
      "ec2:AssociateIamInstanceProfile",
      "ec2:ReplaceIamInstanceProfileAssociation"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:Describe*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "applicationinsights:Describe*",
      "applicationinsights:List*",
      "cloudformation:ListStackResources",
      "cloudformation:DescribeStacks"
    ],
    "Resource" : "*"
  }

```

```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights>DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights>DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups>DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  }
}

```

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ServerMigrationServiceRoleForInstanceValidation

ServerMigrationServiceRoleForInstanceValidation es una [política administrada por AWS](#) que: permite que el SMS de AWS ejecute el script de validación de datos utilizado y devuelva el script correcto o erróneo al SMS

Uso de la política

Puede asociar ServerMigrationServiceRoleForInstanceValidation a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de julio de 2020 a las 22:25 UTC
- Hora de edición: 20 de julio de 2020 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ServiceQuotasFullAccess

ServiceQuotasFullAccess es una [política administrada por AWS](#) que: brinda acceso total a Service Quotas

Uso de la política

Puede asociar ServiceQuotasFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2019 a las 15:44 UTC
- Hora de edición: 4 de febrero de 2021 a las 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",

```

```
    "tag:GetTagValues",
    "servicequotas:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/ServiceQuotaMonitor" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "organizations:ServicePrincipal" : [
        "servicequotas.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "servicequotas.amazonaws.com"
    }
  }
}
]
```

}

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ServiceQuotasReadOnlyAccess

ServiceQuotasReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a Service Quotas

Uso de la política

Puede asociar ServiceQuotasReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 24 de junio de 2019 a las 15:31 UTC
- Hora de edición: 21 de diciembre de 2020 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ServiceQuotasServiceRolePolicy

ServiceQuotasServiceRolePolicy es una [política administrada por AWS](#) que: permite que Service Quotas cree casos de ayuda en su nombre

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de mayo de 2019 a las 20:44 UTC
- Hora de edición: 24 de junio de 2019 a las 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

SimpleWorkflowFullAccess

SimpleWorkflowFullAccess es una [política administrada por AWS](#) que: proporciona acceso total al servicio de configuración de Simple Workflow.

Uso de la política

Puede asociar SimpleWorkflowFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

SupportUser

SupportUser es una [política administrada por AWS](#) que: otorga permisos para solucionar y resolver problemas en una Cuenta de AWS. Esta política también permite al usuario ponerse en contacto con el soporte de AWS para crear y gestionar casos.

Uso de la política

Puede asociar `SupportUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:21 UTC
- Hora de edición: 25 de agosto de 2023 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",

```



```
"cloudfront:List*",
"cloudsearch:Describe*",
"cloudsearch:List*",
"cloudtrail:DescribeTrails",
"cloudtrail:GetTrailStatus",
"cloudtrail:LookupEvents",
"cloudtrail:ListTags",
"cloudtrail:ListPublicKeys",
"cloudwatch:Describe*",
"cloudwatch:Get*",
"cloudwatch:List*",
"codecommit:BatchGetRepositories",
"codecommit:Get*",
"codecommit:List*",
"codedeploy:Batch*",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:AcknowledgeJob",
"codepipeline:AcknowledgeThirdPartyJob",
"codepipeline:ListActionTypes",
"codepipeline:ListPipelines",
"codepipeline:PollForJobs",
"codepipeline:PollForThirdPartyJobs",
"codepipeline:GetPipelineState",
"codepipeline:GetPipeline",
"cognito-identity:List*",
"cognito-identity:LookupDeveloperIdentity",
"cognito-identity:Describe*",
"cognito-idp:DescribeResourceServer",
"cognito-idp:DescribeRiskConfiguration",
"cognito-idp:DescribeUserImportJob",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolDomain",
"cognito-idp:List*",
"cognito-sync:Describe*",
"cognito-sync:GetBulkPublishDetails",
"cognito-sync:GetCognitoEvents",
"cognito-sync:GetIdentityPoolConfiguration",
"cognito-sync:List*",
"config:DescribeConfigurationRecorders",
"config:DescribeConfigurationRecorderStatus",
"config:DescribeConfigRuleEvaluationStatus",
"config:DescribeConfigRules",
"config:DescribeDeliveryChannels",
```

```
"config:DescribeDeliveryChannelStatus",
"config:GetResourceConfigHistory",
"config:ListDiscoveredResources",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:QueryObjects",
"datapipeline:ReportTaskProgress",
"datapipeline:ReportTaskRunnerHeartbeat",
"devicefarm:List*",
"devicefarm:Get*",
"directconnect:Describe*",
"discovery:Describe*",
"discovery:ListConfigurations",
"dms:Describe*",
"dms:List*",
"ds:DescribeDirectories",
"ds:DescribeSnapshots",
"ds:GetDirectoryLimits",
"ds:GetSnapshotLimits",
"ds:ListAuthorizedApplications",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"ec2:Describe*",
"ec2:DescribeHosts",
"ec2:describeIdentityIdFormat",
"ec2:DescribeIdFormat",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeNatGateways",
"ec2:DescribeReservedInstancesModifications",
"ec2:DescribeTags",
"ec2:SearchLocalGatewayRoutes",
"ecr:GetRepositoryPolicy",
"ecr:BatchCheckLayerAvailability",
"ecr:DescribeRepositories",
"ecr:ListImages",
"ecs:Describe*",
"ecs:List*",
"elasticache:Describe*",
"elasticache:List*",
"elasticbeanstalk:Check*",
"elasticbeanstalk:Describe*",
```

```
"elasticbeanstalk:List*",
"elasticbeanstalk:RequestEnvironmentInfo",
"elasticbeanstalk:RetrieveEnvironmentInfo",
"elasticbeanstalk:ValidateConfigurationSettings",
"elasticfilesystem:Describe*",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:List*",
"elastictranscoder:List*",
"elastictranscoder:ReadJob",
"elasticfilesystem:DescribeFileSystems",
"es:Describe*",
"es:List*",
"es:ESHttpGet",
"es:ESHttpHead",
"events:DescribeRule",
"events:List*",
"events:TestEventPattern",
"firehose:Describe*",
"firehose:List*",
"gamelift:List*",
"gamelift:Describe*",
"glacier:ListVaults",
"glacier:DescribeVault",
"glacier:DescribeJob",
"glacier:Get*",
"glacier:List*",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"importexport:GetStatus",
"importexport:ListJobs",
"inspector:Describe*",
"inspector:List*",
"iot:Describe*",
"iot:Get*",
"iot:List*",
"kinesisanalytics:DescribeApplication",
"kinesisanalytics:DiscoverInputSchema",
"kinesisanalytics:GetApplicationState",
"kinesisanalytics:ListApplications",
"kinesis:Describe*",
"kinesis:Get*",
```

```
"kinesis:List*",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lambda:List*",
"lambda:Get*",
"logs:Describe*",
"logs:TestMetricFilter",
"machinelearning:Describe*",
"machinelearning:Get*",
"opsworks:Describe*",
"rds:Describe*",
"rds:ListTagsForResource",
"redshift:Describe*",
"route53:Get*",
"route53:List*",
"route53domains:CheckDomainAvailability",
"route53domains:GetDomainDetail",
"route53domains:GetOperationDetail",
"route53domains:List*",
"s3:List*",
"sdb:GetAttributes",
"sdb:List*",
"sdb:Select*",
"servicecatalog:SearchProducts",
"servicecatalog:DescribeProduct",
"servicecatalog:DescribeProductView",
"servicecatalog:ListLaunchPaths",
"servicecatalog:DescribeProvisioningParameters",
"servicecatalog:ListRecordHistory",
"servicecatalog:DescribeRecord",
"servicecatalog:ScanProvisionedProducts",
"ses:Get*",
"ses:List*",
"sns:Get*",
"sns:List*",
"sqs:GetQueueAttributes",
"sqs:GetQueueUrl",
"sqs:ListQueues",
"sqs:ReceiveMessage",
"ssm:List*",
"ssm:Describe*",
"storagegateway:Describe*",
"storagegateway:List*",
```

```
    "swf:Count*",
    "swf:Describe*",
    "swf:Get*",
    "swf:List*",
    "waf:Get*",
    "waf:List*",
    "workdocs:Describe*",
    "workmail:Describe*",
    "workmail:Get*",
    "workspaces:Describe*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

SystemAdministrator

SystemAdministrator es una [política administrada por AWS](#) que: concede permisos de acceso total necesarios para los recursos que las operaciones de desarrollo y aplicaciones precisan.

Uso de la política

Puede asociar SystemAdministrator a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:23 UTC

- Hora de edición: 24 de agosto de 2020 a las 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
```

```
"codepipeline:*",
"config:*",
"ds:*",
"ec2:Allocate*",
"ec2:AssignPrivateIpAddresses*",
"ec2:Associate*",
"ec2:Allocate*",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AttachVpnGateway",
"ec2:Bundle*",
"ec2:Cancel*",
"ec2:Copy*",
"ec2:CreateCustomerGateway",
"ec2:CreateDhcpOptions",
"ec2:CreateFlowLogs",
"ec2:CreateImage",
"ec2:CreateInstanceExportTask",
"ec2:CreateInternetGateway",
"ec2:CreateKeyPair",
"ec2:CreateLaunchTemplate",
"ec2:CreateLaunchTemplateVersion",
"ec2:CreateNatGateway",
"ec2:CreateNetworkInterface",
"ec2:CreatePlacementGroup",
"ec2:CreateReservedInstancesListing",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSnapshot",
"ec2:CreateSpotDatafeedSubscription",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:CreateVpnConnection",
"ec2:CreateVpnConnectionRoute",
"ec2:CreateVpnGateway",
"ec2>DeleteFlowLogs",
"ec2>DeleteKeyPair",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteLaunchTemplateVersions",
"ec2>DeleteNatGateway",
```

```
"ec2:DeleteNetworkInterface",
"ec2:DeletePlacementGroup",
"ec2:DeleteSnapshot",
"ec2:DeleteSpotDatafeedSubscription",
"ec2:DeleteSubnet",
"ec2:DeleteTags",
"ec2:DeleteVpc",
"ec2:DeleteVpcEndpoints",
"ec2:DeleteVpnConnection",
"ec2:DeleteVpnConnectionRoute",
"ec2:DeleteVpnGateway",
"ec2:DeregisterImage",
"ec2:Describe*",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVpnGateway",
"ec2:DisableVgwRoutePropagation",
"ec2:DisableVpcClassicLinkDnsSupport",
"ec2:DisassociateAddress",
"ec2:DisassociateRouteTable",
"ec2:EnableVgwRoutePropagation",
"ec2:EnableVolumeIO",
"ec2:EnableVpcClassicLinkDnsSupport",
"ec2:GetConsoleOutput",
"ec2:GetHostReservationPurchasePreview",
"ec2:GetLaunchTemplateData",
"ec2:GetPasswordData",
"ec2: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"
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

TranslateFullAccess

TranslateFullAccess es una [política administrada por AWS](#) que: otorga acceso total a Amazon Translate.

Uso de la política

Puede asociar TranslateFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 27 de noviembre de 2018 a las 23:36 UTC
- Hora de edición: 8 de enero de 2020 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "translate:*",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

TranslateReadOnly

TranslateReadOnly es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon Translate.

Uso de la política

Puede asociar TranslateReadOnly a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2017 a las 18:22 UTC
- Hora de edición: 24 de mayo de 2023 a las 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:ListParallelData",

```

```
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

ViewOnlyAccess

ViewOnlyAccess es una [política administrada por AWS](#) que: otorga permisos para ver los recursos y los metadatos básicos en todos los servicios de AWS.

Uso de la política

Puede asociar ViewOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:20 UTC
- Hora de edición: 6 de marzo de 2023 a las 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Versión de la política

Versión de la política: v17 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)

- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

VMImportExportRoleForAWSConnector

`VMImportExportRoleForAWSConnector` es una [política administrada por AWS](#) que: está predeterminada para el rol de servicio de VM Import/Export, para los clientes que utilizan AWS Connector. El servicio VM Import/Export asume un rol con esta política para llevar a cabo las solicitudes de migración de máquinas virtuales desde el dispositivo virtual de AWS Connector. (Tenga en cuenta que AWS Connector utiliza la política administrada “AWSConnector” para emitir solicitudes en nombre del cliente al servicio VM Import/Export). Ofrece la posibilidad de crear capturas de AMI y de EBS, modificar los atributos de las capturas de EBS, realizar llamadas “Describe*” a objetos de EC2 y leer archivos de S3 que comiencen por “import-to-ec2”.

Uso de la política

Puede asociar `VMImportExportRoleForAWSConnector` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 3 de septiembre de 2015 a las 20:48 UTC
- Hora de edición: 3 de septiembre de 2015 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetBucketLocation",
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::import-to-ec2-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifySnapshotAttribute",
      "ec2:CopySnapshot",
      "ec2:RegisterImage",
      "ec2:Describe*"
    ],
    "Resource" : "*"
  }
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

VPCLatticeFullAccess

VPCLatticeFullAccess es una [política administrada por AWS](#) que: brinda acceso total a Amazon VPC Lattice y a los servicios de dependencia.

Uso de la política

Puede asociar `VPCLatticeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de marzo de 2023 a las 02:49 UTC
- Hora de edición: 30 de marzo de 2023 a las 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
```



```

    "firehose:ListDeliveryStreams",
    "logs:DescribeLogGroups",
    "s3:ListAllMyBuckets",
    "lambda:ListAliases",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction"
  ],
  "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"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

VPCLatticeReadOnlyAccess

VPCLatticeReadOnlyAccess es una [política administrada por AWS](#) que: proporciona acceso de solo lectura a Amazon VPC Lattice a través de la AWS Management Console, y acceso limitado a los servicios de dependencia.

Uso de la política

Puede asociar VPCLatticeReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de marzo de 2023 a las 02:47 UTC
- Hora de edición: 30 de marzo de 2023 a las 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
```

```
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
}
]
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

VPCLatticeServicesInvokeAccess

VPCLatticeServicesInvokeAccess es una [política administrada por AWS](#) que: otorga acceso a la invocación de los servicios de Amazon VPC Lattice.

Uso de la política

Puede asociar VPCLatticeServicesInvokeAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 30 de marzo de 2023 a las 02:45 UTC
- Hora de edición: 30 de marzo de 2023 a las 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

WAFLoggingServiceRolePolicy

WAFLoggingServiceRolePolicy es una [política administrada por AWS](#) que: crea SLR para escribir los registros de los clientes en un flujo de firehose

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de agosto de 2018 a las 21:05 UTC
- Hora de edición: 24 de agosto de 2018 a las 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

WAFRegionalLoggingServiceRolePolicy

WAFRegionalLoggingServiceRolePolicy es una [política administrada por AWS](#) que: crea SLR para escribir los registros de los clientes en un flujo de firehose

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de agosto de 2018 a las 18:40 UTC
- Hora de edición: 24 de agosto de 2018 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
```

```
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"  
    ]  
}  
]  
}
```

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

WAFV2LoggingServiceRolePolicy

WAFV2LoggingServiceRolePolicy es una [política administrada por AWS](#) que: crea un rol vinculado a un servicio que permite a AWS WAF escribir registros en Amazon Kinesis Data Firehose.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de noviembre de 2019 a las 00:40 UTC
- Hora de edición: 23 de julio de 2020 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

WellArchitectedConsoleFullAccess

WellArchitectedConsoleFullAccess es una [política administrada por AWS](#) que: proporciona acceso total a la herramienta AWS Well-Architected a través de la AWS Management Console

Uso de la política

Puede asociar WellArchitectedConsoleFullAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2018 a las 18:19 UTC
- Hora de edición: 29 de noviembre de 2018 a las 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

WellArchitectedConsoleReadOnlyAccess

WellArchitectedConsoleReadOnlyAccess es una [política administrada por AWS](#) que: brinda acceso de solo lectura a la herramienta AWS Well-Architected a través de la AWS Management Console

Uso de la política

Puede asociar WellArchitectedConsoleReadOnlyAccess a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 29 de noviembre de 2018 a las 18:21 UTC
- Hora de edición: 29 de junio de 2023 a las 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

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

```
}  
]  
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

WorkLinkServiceRolePolicy

WorkLinkServiceRolePolicy es una [política administrada por AWS](#) que: permite el acceso a Servicios de AWS y a los recursos utilizados o gestionados por Amazon WorkLink

Uso de la política

Puede asociar WorkLinkServiceRolePolicy a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada por AWS
- Hora de creación: 23 de enero de 2019 a las 19:03 UTC
- Hora de edición: 23 de enero de 2019 a las 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita acceso a un recurso de AWS, AWS comprueba la versión predeterminada de la política para decidir si permite o no la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"
    }
  ]
}
```

Más información

- [Cree un conjunto de permisos mediante el uso de las políticas administradas por AWS en el Centro de identidades de IAM](#)
- [Adición y eliminación de permisos de identidad de IAM](#)
- [Conozca el control de versiones de las políticas de IAM](#)
- [Introducción a las políticas administradas por AWS y el objetivo de los permisos de privilegio mínimo](#)

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.