



Guida di riferimento

AWS Policy gestita



AWS Policy gestita: Guida di riferimento

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

| | |
|--|----|
| Cosa sono le policy AWS gestite? | 1 |
| Comprendere le pagine di riferimento delle politiche | 1 |
| Policy gestite da AWS obsolete | 2 |
| AWS politiche gestite | 3 |
| AccessAnalyzerServiceRolePolicy | 44 |
| Utilizzo di questa politica | 44 |
| Dettagli della politica | 44 |
| Versione della politica | 44 |
| Documento di policy JSON | 45 |
| Ulteriori informazioni | 47 |
| AdministratorAccess | 47 |
| Utilizzo di questa politica | 47 |
| Dettagli della politica | 47 |
| Versione della politica | 48 |
| Documento di policy JSON | 48 |
| Ulteriori informazioni | 48 |
| AdministratorAccess-Amplify | 48 |
| Utilizzo di questa politica | 48 |
| Dettagli della politica | 49 |
| Versione della politica | 49 |
| Documento di policy JSON | 49 |
| Ulteriori informazioni | 59 |
| AdministratorAccess-AWSElasticBeanstalk | 60 |
| Utilizzo di questa politica | 60 |
| Dettagli della politica | 60 |
| Versione della politica | 60 |
| Documento di policy JSON | 60 |
| Ulteriori informazioni | 68 |
| AlexaForBusinessDeviceSetup | 69 |
| Utilizzo di questa politica | 69 |
| Dettagli della politica | 69 |
| Versione della politica | 69 |
| Documento di policy JSON | 69 |
| Ulteriori informazioni | 70 |

| | |
|---|----|
| AlexaForBusinessFullAccess | 70 |
| Utilizzo di questa politica | 70 |
| Dettagli della politica | 70 |
| Versione della politica | 71 |
| Documento di policy JSON | 71 |
| Ulteriori informazioni | 72 |
| AlexaForBusinessGatewayExecution | 72 |
| Utilizzo di questa politica | 73 |
| Dettagli della politica | 73 |
| Versione della politica | 73 |
| Documento di policy JSON | 73 |
| Ulteriori informazioni | 74 |
| AlexaForBusinessLifesizeDelegatedAccessPolicy | 74 |
| Utilizzo di questa politica | 74 |
| Dettagli della politica | 74 |
| Versione della politica | 75 |
| Documento di policy JSON | 75 |
| Ulteriori informazioni | 77 |
| AlexaForBusinessNetworkProfileServicePolicy | 77 |
| Utilizzo di questa politica | 78 |
| Dettagli della politica | 78 |
| Versione della politica | 78 |
| Documento di policy JSON | 78 |
| Ulteriori informazioni | 79 |
| AlexaForBusinessPolyDelegatedAccessPolicy | 79 |
| Utilizzo di questa politica | 79 |
| Dettagli della politica | 79 |
| Versione della politica | 79 |
| Documento di policy JSON | 80 |
| Ulteriori informazioni | 81 |
| AlexaForBusinessReadOnlyAccess | 82 |
| Utilizzo di questa politica | 82 |
| Dettagli della politica | 82 |
| Versione della politica | 82 |
| Documento di policy JSON | 82 |
| Ulteriori informazioni | 83 |

| | |
|--|----|
| AmazonAPIGatewayAdministrator | 83 |
| Utilizzo di questa politica | 83 |
| Dettagli della politica | 83 |
| Versione della politica | 83 |
| Documento di policy JSON | 84 |
| Ulteriori informazioni | 84 |
| AmazonAPIGatewayInvokeFullAccess | 84 |
| Utilizzo di questa politica | 84 |
| Dettagli della politica | 84 |
| Versione della politica | 85 |
| Documento di policy JSON | 85 |
| Ulteriori informazioni | 85 |
| AmazonAPIGatewayPushToCloudWatchLogs | 85 |
| Utilizzo di questa politica | 86 |
| Dettagli della politica | 86 |
| Versione della politica | 86 |
| Documento di policy JSON | 86 |
| Ulteriori informazioni | 87 |
| AmazonAppFlowFullAccess | 87 |
| Utilizzo di questa politica | 87 |
| Dettagli della politica | 87 |
| Versione della politica | 87 |
| Documento di policy JSON | 88 |
| Ulteriori informazioni | 90 |
| AmazonAppFlowReadOnlyAccess | 91 |
| Utilizzo di questa politica | 91 |
| Dettagli della politica | 91 |
| Versione della politica | 91 |
| Documento di policy JSON | 91 |
| Ulteriori informazioni | 92 |
| AmazonAppStreamFullAccess | 92 |
| Utilizzo di questa politica | 92 |
| Dettagli della politica | 92 |
| Versione della politica | 92 |
| Documento di policy JSON | 93 |
| Ulteriori informazioni | 94 |

| | |
|--|-----|
| AmazonAppStreamPCAAccess | 95 |
| Utilizzo di questa politica | 95 |
| Dettagli della politica | 95 |
| Versione della politica | 95 |
| Documento di policy JSON | 95 |
| Ulteriori informazioni | 96 |
| AmazonAppStreamReadOnlyAccess | 96 |
| Utilizzo di questa politica | 96 |
| Dettagli della politica | 96 |
| Versione della politica | 97 |
| Documento di policy JSON | 97 |
| Ulteriori informazioni | 97 |
| AmazonAppStreamServiceAccess | 97 |
| Utilizzo di questa politica | 98 |
| Dettagli della politica | 98 |
| Versione della politica | 98 |
| Documento di policy JSON | 98 |
| Ulteriori informazioni | 99 |
| AmazonAthenaFullAccess | 99 |
| Utilizzo di questa politica | 100 |
| Dettagli della politica | 100 |
| Versione della politica | 100 |
| Documento di policy JSON | 100 |
| Ulteriori informazioni | 103 |
| AmazonAugmentedAIFullAccess | 104 |
| Utilizzo di questa politica | 104 |
| Dettagli della politica | 104 |
| Versione della politica | 104 |
| Documento di policy JSON | 104 |
| Ulteriori informazioni | 105 |
| AmazonAugmentedAIHumanLoopFullAccess | 106 |
| Utilizzo di questa politica | 106 |
| Dettagli della politica | 106 |
| Versione della politica | 106 |
| Documento di policy JSON | 106 |
| Ulteriori informazioni | 107 |

| | |
|---|-----|
| AmazonAugmentedAllIntegratedAPIAccess | 107 |
| Utilizzo di questa politica | 107 |
| Dettagli della politica | 107 |
| Versione della politica | 107 |
| Documento di policy JSON | 108 |
| Ulteriori informazioni | 109 |
| AmazonBedrockFullAccess | 109 |
| Utilizzo di questa politica | 109 |
| Dettagli della politica | 109 |
| Versione della politica | 110 |
| Documento di policy JSON | 110 |
| Ulteriori informazioni | 111 |
| AmazonBedrockReadOnly | 111 |
| Utilizzo di questa politica | 111 |
| Dettagli della politica | 111 |
| Versione della politica | 112 |
| Documento di policy JSON | 112 |
| Ulteriori informazioni | 112 |
| AmazonBraketFullAccess | 113 |
| Utilizzo di questa politica | 113 |
| Dettagli della politica | 113 |
| Versione della politica | 113 |
| Documento di policy JSON | 113 |
| Ulteriori informazioni | 117 |
| AmazonBraketJobsExecutionPolicy | 118 |
| Utilizzo di questa politica | 118 |
| Dettagli della politica | 118 |
| Versione della politica | 118 |
| Documento di policy JSON | 118 |
| Ulteriori informazioni | 121 |
| AmazonBraketServiceRolePolicy | 121 |
| Utilizzo di questa politica | 121 |
| Dettagli della politica | 121 |
| Versione della politica | 121 |
| Documento di policy JSON | 122 |
| Ulteriori informazioni | 122 |

| | |
|---|-----|
| AmazonChimeFullAccess | 123 |
| Utilizzo di questa politica | 123 |
| Dettagli della politica | 123 |
| Versione della politica | 123 |
| Documento di policy JSON | 123 |
| Ulteriori informazioni | 125 |
| AmazonChimeReadOnly | 126 |
| Utilizzo di questa politica | 126 |
| Dettagli della politica | 126 |
| Versione della politica | 126 |
| Documento di policy JSON | 126 |
| Ulteriori informazioni | 127 |
| AmazonChimeSDK | 127 |
| Utilizzo di questa politica | 127 |
| Dettagli della politica | 127 |
| Versione della politica | 127 |
| Documento di policy JSON | 128 |
| Ulteriori informazioni | 129 |
| AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy | 129 |
| Utilizzo di questa politica | 129 |
| Dettagli della politica | 129 |
| Versione della politica | 129 |
| Documento di policy JSON | 129 |
| Ulteriori informazioni | 131 |
| AmazonChimeSDKMessagingServiceRolePolicy | 131 |
| Utilizzo di questa politica | 131 |
| Dettagli della politica | 131 |
| Versione della politica | 131 |
| Documento di policy JSON | 132 |
| Ulteriori informazioni | 132 |
| AmazonChimeServiceRolePolicy | 132 |
| Utilizzo di questa politica | 133 |
| Dettagli della politica | 133 |
| Versione della politica | 133 |
| Documento di policy JSON | 133 |
| Ulteriori informazioni | 134 |

| | |
|--|-----|
| AmazonChimeTranscriptionServiceLinkedRolePolicy | 134 |
| Utilizzo di questa politica | 134 |
| Dettagli della politica | 134 |
| Versione della politica | 134 |
| Documento di policy JSON | 135 |
| Ulteriori informazioni | 135 |
| AmazonChimeUserManagement | 135 |
| Utilizzo di questa politica | 135 |
| Dettagli della politica | 135 |
| Versione della politica | 136 |
| Documento di policy JSON | 136 |
| Ulteriori informazioni | 137 |
| AmazonChimeVoiceConnectorServiceLinkedRolePolicy | 137 |
| Utilizzo di questa politica | 137 |
| Dettagli della politica | 137 |
| Versione della politica | 138 |
| Documento di policy JSON | 138 |
| Ulteriori informazioni | 140 |
| AmazonCloudDirectoryFullAccess | 140 |
| Utilizzo di questa politica | 140 |
| Dettagli della politica | 140 |
| Versione della politica | 140 |
| Documento di policy JSON | 140 |
| Ulteriori informazioni | 141 |
| AmazonCloudDirectoryReadOnlyAccess | 141 |
| Utilizzo di questa politica | 141 |
| Dettagli della politica | 141 |
| Versione della politica | 142 |
| Documento di policy JSON | 142 |
| Ulteriori informazioni | 142 |
| AmazonCloudWatchEvidentlyFullAccess | 142 |
| Utilizzo di questa politica | 143 |
| Dettagli della politica | 143 |
| Versione della politica | 143 |
| Documento di policy JSON | 143 |
| Ulteriori informazioni | 146 |

| | |
|--|-----|
| AmazonCloudWatchEvidentlyReadOnlyAccess | 146 |
| Utilizzo di questa politica | 146 |
| Dettagli della politica | 146 |
| Versione della politica | 146 |
| Documento di policy JSON | 146 |
| Ulteriori informazioni | 147 |
| AmazonCloudWatchEvidentlyServiceRolePolicy | 147 |
| Utilizzo di questa politica | 147 |
| Dettagli della politica | 147 |
| Versione della politica | 148 |
| Documento di policy JSON | 148 |
| Ulteriori informazioni | 149 |
| AmazonCloudWatchRUMFullAccess | 149 |
| Utilizzo di questa politica | 150 |
| Dettagli della politica | 150 |
| Versione della politica | 150 |
| Documento di policy JSON | 150 |
| Ulteriori informazioni | 153 |
| AmazonCloudWatchRUMReadOnlyAccess | 153 |
| Utilizzo di questa politica | 153 |
| Dettagli della politica | 153 |
| Versione della politica | 153 |
| Documento di policy JSON | 153 |
| Ulteriori informazioni | 154 |
| AmazonCloudWatchRUMServiceRolePolicy | 154 |
| Utilizzo di questa politica | 154 |
| Dettagli della politica | 154 |
| Versione della politica | 155 |
| Documento di policy JSON | 155 |
| Ulteriori informazioni | 156 |
| AmazonCodeCatalystFullAccess | 156 |
| Utilizzo di questa politica | 156 |
| Dettagli della politica | 156 |
| Versione della politica | 156 |
| Documento di policy JSON | 156 |
| Ulteriori informazioni | 157 |

| | |
|--|-----|
| AmazonCodeCatalystReadOnlyAccess | 157 |
| Utilizzo di questa politica | 157 |
| Dettagli della politica | 158 |
| Versione della politica | 158 |
| Documento di policy JSON | 158 |
| Ulteriori informazioni | 158 |
| AmazonCodeCatalystSupportAccess | 159 |
| Utilizzo di questa politica | 159 |
| Dettagli della politica | 159 |
| Versione della politica | 159 |
| Documento di policy JSON | 159 |
| Ulteriori informazioni | 160 |
| AmazonCodeGuruProfilerAgentAccess | 160 |
| Utilizzo di questa politica | 160 |
| Dettagli della politica | 160 |
| Versione della politica | 161 |
| Documento di policy JSON | 161 |
| Ulteriori informazioni | 161 |
| AmazonCodeGuruProfilerFullAccess | 161 |
| Utilizzo di questa politica | 162 |
| Dettagli della politica | 162 |
| Versione della politica | 162 |
| Documento di policy JSON | 162 |
| Ulteriori informazioni | 163 |
| AmazonCodeGuruProfilerReadOnlyAccess | 163 |
| Utilizzo di questa politica | 163 |
| Dettagli della politica | 163 |
| Versione della politica | 163 |
| Documento di policy JSON | 164 |
| Ulteriori informazioni | 164 |
| AmazonCodeGuruReviewerFullAccess | 164 |
| Utilizzo di questa politica | 165 |
| Dettagli della politica | 165 |
| Versione della politica | 165 |
| Documento di policy JSON | 165 |
| Ulteriori informazioni | 168 |

| | |
|---|-----|
| AmazonCodeGuruReviewerReadOnlyAccess | 168 |
| Utilizzo di questa politica | 168 |
| Dettagli della politica | 168 |
| Versione della politica | 168 |
| Documento di policy JSON | 168 |
| Ulteriori informazioni | 169 |
| AmazonCodeGuruReviewerServiceRolePolicy | 169 |
| Utilizzo di questa politica | 169 |
| Dettagli della politica | 169 |
| Versione della politica | 170 |
| Documento di policy JSON | 170 |
| Ulteriori informazioni | 172 |
| AmazonCodeGuruSecurityFullAccess | 172 |
| Utilizzo di questa politica | 172 |
| Dettagli della politica | 172 |
| Versione della politica | 172 |
| Documento di policy JSON | 173 |
| Ulteriori informazioni | 173 |
| AmazonCodeGuruSecurityScanAccess | 173 |
| Utilizzo di questa politica | 173 |
| Dettagli della politica | 174 |
| Versione della politica | 174 |
| Documento di policy JSON | 174 |
| Ulteriori informazioni | 174 |
| AmazonCognitoDeveloperAuthenticatedIdentities | 175 |
| Utilizzo di questa politica | 175 |
| Dettagli della politica | 175 |
| Versione della politica | 175 |
| Documento di policy JSON | 175 |
| Ulteriori informazioni | 176 |
| AmazonCognitoIdpEmailServiceRolePolicy | 176 |
| Utilizzo di questa politica | 176 |
| Dettagli della politica | 176 |
| Versione della politica | 177 |
| Documento di policy JSON | 177 |
| Ulteriori informazioni | 177 |

| | |
|--|-----|
| AmazonCognitoIdpServiceRolePolicy | 177 |
| Utilizzo di questa politica | 178 |
| Dettagli della politica | 178 |
| Versione della politica | 178 |
| Documento di policy JSON | 178 |
| Ulteriori informazioni | 179 |
| AmazonCognitoPowerUser | 179 |
| Utilizzo di questa politica | 179 |
| Dettagli della politica | 179 |
| Versione della politica | 179 |
| Documento di policy JSON | 179 |
| Ulteriori informazioni | 181 |
| AmazonCognitoReadOnly | 181 |
| Utilizzo di questa politica | 181 |
| Dettagli della politica | 181 |
| Versione della politica | 181 |
| Documento di policy JSON | 182 |
| Ulteriori informazioni | 182 |
| AmazonCognitoUnAuthedIdentitiesSessionPolicy | 182 |
| Utilizzo di questa politica | 183 |
| Dettagli della politica | 183 |
| Versione della politica | 183 |
| Documento di policy JSON | 183 |
| Ulteriori informazioni | 184 |
| AmazonCognitoUnauthenticatedIdentities | 184 |
| Utilizzo di questa politica | 184 |
| Dettagli della politica | 184 |
| Versione della politica | 185 |
| Documento di policy JSON | 185 |
| Ulteriori informazioni | 185 |
| AmazonConnect_FullAccess | 185 |
| Utilizzo di questa politica | 186 |
| Dettagli della politica | 186 |
| Versione della politica | 186 |
| Documento di policy JSON | 186 |
| Ulteriori informazioni | 189 |

| | |
|---|-----|
| AmazonConnectCampaignsServiceLinkedRolePolicy | 189 |
| Utilizzo di questa politica | 189 |
| Dettagli della politica | 189 |
| Versione della politica | 189 |
| Documento di policy JSON | 190 |
| Ulteriori informazioni | 190 |
| AmazonConnectReadOnlyAccess | 190 |
| Utilizzo di questa politica | 191 |
| Dettagli della politica | 191 |
| Versione della politica | 191 |
| Documento di policy JSON | 191 |
| Ulteriori informazioni | 192 |
| AmazonConnectServiceLinkedRolePolicy | 192 |
| Utilizzo di questa politica | 192 |
| Dettagli della politica | 192 |
| Versione della politica | 192 |
| Documento di policy JSON | 193 |
| Ulteriori informazioni | 198 |
| AmazonConnectSynchronizationServiceRolePolicy | 198 |
| Utilizzo di questa politica | 198 |
| Dettagli della politica | 198 |
| Versione della politica | 198 |
| Documento di policy JSON | 199 |
| Ulteriori informazioni | 201 |
| AmazonConnectVoiceIDFullAccess | 201 |
| Utilizzo di questa politica | 201 |
| Dettagli della politica | 201 |
| Versione della politica | 201 |
| Documento di policy JSON | 201 |
| Ulteriori informazioni | 202 |
| AmazonDataZoneDomainExecutionRolePolicy | 202 |
| Utilizzo di questa politica | 202 |
| Dettagli della politica | 202 |
| Versione della politica | 203 |
| Documento di policy JSON | 203 |
| Ulteriori informazioni | 206 |

| | |
|--|-----|
| AmazonDataZoneEnvironmentRolePermissionsBoundary | 206 |
| Utilizzo di questa politica | 206 |
| Dettagli della politica | 206 |
| Versione della politica | 206 |
| Documento di policy JSON | 207 |
| Ulteriori informazioni | 219 |
| AmazonDataZoneFullAccess | 220 |
| Utilizzo di questa politica | 220 |
| Dettagli della politica | 220 |
| Versione della politica | 220 |
| Documento di policy JSON | 220 |
| Ulteriori informazioni | 224 |
| AmazonDataZoneFullUserAccess | 224 |
| Utilizzo di questa politica | 224 |
| Dettagli della politica | 224 |
| Versione della politica | 224 |
| Documento di policy JSON | 225 |
| Ulteriori informazioni | 227 |
| AmazonDataZoneGlueManageAccessRolePolicy | 228 |
| Utilizzo di questa politica | 228 |
| Dettagli della politica | 228 |
| Versione della politica | 228 |
| Documento di policy JSON | 228 |
| Ulteriori informazioni | 233 |
| AmazonDataZonePortalFullAccessPolicy | 233 |
| Utilizzo di questa politica | 234 |
| Dettagli della politica | 234 |
| Versione della politica | 234 |
| Documento di policy JSON | 234 |
| Ulteriori informazioni | 234 |
| AmazonDataZonePreviewConsoleFullAccess | 235 |
| Utilizzo di questa politica | 235 |
| Dettagli della politica | 235 |
| Versione della politica | 235 |
| Documento di policy JSON | 235 |
| Ulteriori informazioni | 237 |

| | |
|---|-----|
| AmazonDataZoneProjectDeploymentPermissionsBoundary | 237 |
| Utilizzo di questa politica | 237 |
| Dettagli della politica | 238 |
| Versione della politica | 238 |
| Documento di policy JSON | 238 |
| Ulteriori informazioni | 246 |
| AmazonDataZoneProjectRolePermissionsBoundary | 246 |
| Utilizzo di questa politica | 246 |
| Dettagli della politica | 246 |
| Versione della politica | 247 |
| Documento di policy JSON | 247 |
| Ulteriori informazioni | 254 |
| AmazonDataZoneRedshiftGlueProvisioningPolicy | 254 |
| Utilizzo di questa politica | 254 |
| Dettagli della politica | 255 |
| Versione della politica | 255 |
| Documento di policy JSON | 255 |
| Ulteriori informazioni | 263 |
| AmazonDataZoneRedshiftManageAccessRolePolicy | 263 |
| Utilizzo di questa politica | 263 |
| Dettagli della politica | 263 |
| Versione della politica | 263 |
| Documento di policy JSON | 264 |
| Ulteriori informazioni | 266 |
| AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary | 266 |
| Utilizzo di questa politica | 266 |
| Dettagli della politica | 266 |
| Versione della politica | 267 |
| Documento di policy JSON | 267 |
| Ulteriori informazioni | 294 |
| AmazonDataZoneSageMakerManageAccessRolePolicy | 294 |
| Utilizzo di questa politica | 294 |
| Dettagli della politica | 294 |
| Versione della politica | 295 |
| Documento di policy JSON | 295 |
| Ulteriori informazioni | 299 |

| | |
|---|-----|
| AmazonDataZoneSageMakerProvisioningRolePolicy | 300 |
| Utilizzo di questa politica | 300 |
| Dettagli della politica | 300 |
| Versione della politica | 300 |
| Documento di policy JSON | 300 |
| Ulteriori informazioni | 305 |
| AmazonDetectiveFullAccess | 305 |
| Utilizzo di questa politica | 305 |
| Dettagli della politica | 305 |
| Versione della politica | 306 |
| Documento di policy JSON | 306 |
| Ulteriori informazioni | 307 |
| AmazonDetectiveInvestigatorAccess | 307 |
| Utilizzo di questa politica | 307 |
| Dettagli della politica | 307 |
| Versione della politica | 307 |
| Documento di policy JSON | 308 |
| Ulteriori informazioni | 309 |
| AmazonDetectiveMemberAccess | 309 |
| Utilizzo di questa politica | 310 |
| Dettagli della politica | 310 |
| Versione della politica | 310 |
| Documento di policy JSON | 310 |
| Ulteriori informazioni | 311 |
| AmazonDetectiveOrganizationsAccess | 311 |
| Utilizzo di questa politica | 311 |
| Dettagli della politica | 311 |
| Versione della politica | 311 |
| Documento di policy JSON | 312 |
| Ulteriori informazioni | 313 |
| AmazonDetectiveServiceLinkedRolePolicy | 313 |
| Utilizzo di questa politica | 314 |
| Dettagli della politica | 314 |
| Versione della politica | 314 |
| Documento di policy JSON | 314 |
| Ulteriori informazioni | 315 |

| | |
|---|-----|
| AmazonDevOpsGuruConsoleFullAccess | 315 |
| Utilizzo di questa politica | 315 |
| Dettagli della politica | 315 |
| Versione della politica | 315 |
| Documento di policy JSON | 315 |
| Ulteriori informazioni | 318 |
| AmazonDevOpsGuruFullAccess | 318 |
| Utilizzo di questa politica | 318 |
| Dettagli della politica | 318 |
| Versione della politica | 318 |
| Documento di policy JSON | 319 |
| Ulteriori informazioni | 321 |
| AmazonDevOpsGuruOrganizationsAccess | 321 |
| Utilizzo di questa politica | 321 |
| Dettagli della politica | 321 |
| Versione della politica | 322 |
| Documento di policy JSON | 322 |
| Ulteriori informazioni | 323 |
| AmazonDevOpsGuruReadOnlyAccess | 323 |
| Utilizzo di questa politica | 323 |
| Dettagli della politica | 323 |
| Versione della politica | 324 |
| Documento di policy JSON | 324 |
| Ulteriori informazioni | 326 |
| AmazonDevOpsGuruServiceRolePolicy | 326 |
| Utilizzo di questa politica | 326 |
| Dettagli della politica | 326 |
| Versione della politica | 326 |
| Documento di policy JSON | 327 |
| Ulteriori informazioni | 331 |
| AmazonDMSCloudWatchLogsRole | 331 |
| Utilizzo di questa politica | 331 |
| Dettagli della politica | 331 |
| Versione della politica | 331 |
| Documento di policy JSON | 331 |
| Ulteriori informazioni | 333 |

| | |
|--|-----|
| AmazonDMSRedshiftS3Role | 333 |
| Utilizzo di questa politica | 333 |
| Dettagli della politica | 333 |
| Versione della politica | 334 |
| Documento di policy JSON | 334 |
| Ulteriori informazioni | 334 |
| AmazonDMSVPCManagementRole | 335 |
| Utilizzo di questa politica | 335 |
| Dettagli della politica | 335 |
| Versione della politica | 335 |
| Documento di policy JSON | 335 |
| Ulteriori informazioni | 336 |
| AmazonDocDB-ElasticServiceRolePolicy | 336 |
| Utilizzo di questa politica | 336 |
| Dettagli della politica | 336 |
| Versione della politica | 337 |
| Documento di policy JSON | 337 |
| Ulteriori informazioni | 337 |
| AmazonDocDBConsoleFullAccess | 337 |
| Utilizzo di questa politica | 338 |
| Dettagli della politica | 338 |
| Versione della politica | 338 |
| Documento di policy JSON | 338 |
| Ulteriori informazioni | 342 |
| AmazonDocDBElasticFullAccess | 343 |
| Utilizzo di questa politica | 343 |
| Dettagli della politica | 343 |
| Versione della politica | 343 |
| Documento di policy JSON | 343 |
| Ulteriori informazioni | 346 |
| AmazonDocDBElasticReadOnlyAccess | 346 |
| Utilizzo di questa politica | 346 |
| Dettagli della politica | 347 |
| Versione della politica | 347 |
| Documento di policy JSON | 347 |
| Ulteriori informazioni | 348 |

| | |
|--|-----|
| AmazonDocDBFullAccess | 348 |
| Utilizzo di questa politica | 348 |
| Dettagli della politica | 348 |
| Versione della politica | 348 |
| Documento di policy JSON | 349 |
| Ulteriori informazioni | 351 |
| AmazonDocDBReadOnlyAccess | 351 |
| Utilizzo di questa politica | 352 |
| Dettagli della politica | 352 |
| Versione della politica | 352 |
| Documento di policy JSON | 352 |
| Ulteriori informazioni | 354 |
| AmazonDRSVPCManagement | 354 |
| Utilizzo di questa politica | 354 |
| Dettagli della politica | 354 |
| Versione della politica | 355 |
| Documento di policy JSON | 355 |
| Ulteriori informazioni | 355 |
| AmazonDynamoDBFullAccess | 356 |
| Utilizzo di questa politica | 356 |
| Dettagli della politica | 356 |
| Versione della politica | 356 |
| Documento di policy JSON | 356 |
| Ulteriori informazioni | 359 |
| AmazonDynamoDBFullAccesswithDataPipeline | 359 |
| Utilizzo di questa politica | 359 |
| Dettagli della politica | 359 |
| Versione della politica | 360 |
| Documento di policy JSON | 360 |
| Ulteriori informazioni | 362 |
| AmazonDynamoDBReadOnlyAccess | 362 |
| Utilizzo di questa politica | 362 |
| Dettagli della politica | 362 |
| Versione della politica | 362 |
| Documento di policy JSON | 363 |
| Ulteriori informazioni | 364 |

| | |
|--|-----|
| AmazonEBSCSIDriverPolicy | 365 |
| Utilizzo di questa politica | 365 |
| Dettagli della politica | 365 |
| Versione della politica | 365 |
| Documento di policy JSON | 365 |
| Ulteriori informazioni | 368 |
| AmazonEC2ContainerRegistryFullAccess | 369 |
| Utilizzo di questa politica | 369 |
| Dettagli della politica | 369 |
| Versione della politica | 369 |
| Documento di policy JSON | 369 |
| Ulteriori informazioni | 370 |
| AmazonEC2ContainerRegistryPowerUser | 370 |
| Utilizzo di questa politica | 370 |
| Dettagli della politica | 370 |
| Versione della politica | 371 |
| Documento di policy JSON | 371 |
| Ulteriori informazioni | 371 |
| AmazonEC2ContainerRegistryReadOnly | 372 |
| Utilizzo di questa politica | 372 |
| Dettagli della politica | 372 |
| Versione della politica | 372 |
| Documento di policy JSON | 372 |
| Ulteriori informazioni | 373 |
| AmazonEC2ContainerServiceAutoscaleRole | 373 |
| Utilizzo di questa politica | 373 |
| Dettagli della politica | 373 |
| Versione della politica | 374 |
| Documento di policy JSON | 374 |
| Ulteriori informazioni | 374 |
| AmazonEC2ContainerServiceEventsRole | 375 |
| Utilizzo di questa politica | 375 |
| Dettagli della politica | 375 |
| Versione della politica | 375 |
| Documento di policy JSON | 375 |
| Ulteriori informazioni | 376 |

| | |
|--|-----|
| AmazonEC2ContainerServiceforEC2Role | 376 |
| Utilizzo di questa politica | 377 |
| Dettagli della politica | 377 |
| Versione della politica | 377 |
| Documento di policy JSON | 377 |
| Ulteriori informazioni | 378 |
| AmazonEC2ContainerServiceRole | 378 |
| Utilizzo di questa politica | 378 |
| Dettagli della politica | 379 |
| Versione della politica | 379 |
| Documento di policy JSON | 379 |
| Ulteriori informazioni | 379 |
| AmazonEC2FullAccess | 380 |
| Utilizzo di questa politica | 380 |
| Dettagli della politica | 380 |
| Versione della politica | 380 |
| Documento di policy JSON | 380 |
| Ulteriori informazioni | 381 |
| AmazonEC2ReadOnlyAccess | 382 |
| Utilizzo di questa politica | 382 |
| Dettagli della politica | 382 |
| Versione della politica | 382 |
| Documento di policy JSON | 382 |
| Ulteriori informazioni | 383 |
| AmazonEC2RoleforAWSCodeDeploy | 383 |
| Utilizzo di questa politica | 383 |
| Dettagli della politica | 383 |
| Versione della politica | 384 |
| Documento di policy JSON | 384 |
| Ulteriori informazioni | 384 |
| AmazonEC2RoleforAWSCodeDeployLimited | 385 |
| Utilizzo di questa politica | 385 |
| Dettagli della politica | 385 |
| Versione della politica | 385 |
| Documento di policy JSON | 385 |
| Ulteriori informazioni | 386 |

| | |
|--|-----|
| AmazonEC2RoleforDataPipelineRole | 386 |
| Utilizzo di questa politica | 386 |
| Dettagli della politica | 386 |
| Versione della politica | 387 |
| Documento di policy JSON | 387 |
| Ulteriori informazioni | 388 |
| AmazonEC2RoleforSSM | 388 |
| Utilizzo di questa politica | 388 |
| Dettagli della politica | 388 |
| Versione della politica | 388 |
| Documento di policy JSON | 389 |
| Ulteriori informazioni | 391 |
| AmazonEC2RolePolicyForLaunchWizard | 391 |
| Utilizzo di questa politica | 391 |
| Dettagli della politica | 391 |
| Versione della politica | 391 |
| Documento di policy JSON | 392 |
| Ulteriori informazioni | 396 |
| AmazonEC2SpotFleetAutoscaleRole | 396 |
| Utilizzo di questa politica | 396 |
| Dettagli della politica | 396 |
| Versione della politica | 396 |
| Documento di policy JSON | 396 |
| Ulteriori informazioni | 397 |
| AmazonEC2SpotFleetTaggingRole | 398 |
| Utilizzo di questa politica | 398 |
| Dettagli della politica | 398 |
| Versione della politica | 398 |
| Documento di policy JSON | 398 |
| Ulteriori informazioni | 400 |
| AmazonECS_FullAccess | 400 |
| Utilizzo di questa politica | 400 |
| Dettagli della politica | 400 |
| Versione della politica | 400 |
| Documento di policy JSON | 400 |
| Ulteriori informazioni | 406 |

| | |
|--|-----|
| AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity | 406 |
| Utilizzo di questa politica | 406 |
| Dettagli della politica | 406 |
| Versione della politica | 407 |
| Documento di policy JSON | 407 |
| Ulteriori informazioni | 409 |
| AmazonECSInfrastructureRolePolicyForVolumes | 409 |
| Utilizzo di questa politica | 409 |
| Dettagli della politica | 409 |
| Versione della politica | 410 |
| Documento di policy JSON | 410 |
| Ulteriori informazioni | 412 |
| AmazonECSServiceRolePolicy | 412 |
| Utilizzo di questa politica | 412 |
| Dettagli della politica | 412 |
| Versione della politica | 412 |
| Documento di policy JSON | 413 |
| Ulteriori informazioni | 417 |
| AmazonECSTaskExecutionRolePolicy | 417 |
| Utilizzo di questa politica | 418 |
| Dettagli della politica | 418 |
| Versione della politica | 418 |
| Documento di policy JSON | 418 |
| Ulteriori informazioni | 419 |
| AmazonEFSCSIDriverPolicy | 419 |
| Utilizzo di questa politica | 419 |
| Dettagli della politica | 419 |
| Versione della politica | 419 |
| Documento di policy JSON | 419 |
| Ulteriori informazioni | 421 |
| AmazonEKS_CNI_Policy | 421 |
| Utilizzo di questa politica | 421 |
| Dettagli della politica | 422 |
| Versione della politica | 422 |
| Documento di policy JSON | 422 |
| Ulteriori informazioni | 423 |

| | |
|--|-----|
| AmazonEKSClusterPolicy | 423 |
| Utilizzo di questa politica | 423 |
| Dettagli della politica | 423 |
| Versione della politica | 424 |
| Documento di policy JSON | 424 |
| Ulteriori informazioni | 426 |
| AmazonEKSConNECTorServiceRolePolicy | 426 |
| Utilizzo di questa politica | 426 |
| Dettagli della politica | 426 |
| Versione della politica | 426 |
| Documento di policy JSON | 427 |
| Ulteriori informazioni | 428 |
| AmazonEKSFargatePodExecutionRolePolicy | 429 |
| Utilizzo di questa politica | 429 |
| Dettagli della politica | 429 |
| Versione della politica | 429 |
| Documento di policy JSON | 429 |
| Ulteriori informazioni | 430 |
| AmazonEKSFoRfargateServiceRolePolicy | 430 |
| Utilizzo di questa politica | 430 |
| Dettagli della politica | 430 |
| Versione della politica | 430 |
| Documento di policy JSON | 431 |
| Ulteriori informazioni | 431 |
| AmazonEKSLocalOutpostClusterPolicy | 431 |
| Utilizzo di questa politica | 432 |
| Dettagli della politica | 432 |
| Versione della politica | 432 |
| Documento di policy JSON | 432 |
| Ulteriori informazioni | 434 |
| AmazonEKSLocalOutpostServiceRolePolicy | 434 |
| Utilizzo di questa politica | 434 |
| Dettagli della politica | 434 |
| Versione della politica | 435 |
| Documento di policy JSON | 435 |
| Ulteriori informazioni | 440 |

| | |
|---------------------------------------|-----|
| AmazonEKSServicePolicy | 440 |
| Utilizzo di questa politica | 441 |
| Dettagli della politica | 441 |
| Versione della politica | 441 |
| Documento di policy JSON | 441 |
| Ulteriori informazioni | 443 |
| AmazonEKSServiceRolePolicy | 443 |
| Utilizzo di questa politica | 443 |
| Dettagli della politica | 443 |
| Versione della politica | 443 |
| Documento di policy JSON | 444 |
| Ulteriori informazioni | 446 |
| AmazonEKSVPCResourceController | 446 |
| Utilizzo di questa politica | 446 |
| Dettagli della politica | 446 |
| Versione della politica | 447 |
| Documento di policy JSON | 447 |
| Ulteriori informazioni | 447 |
| AmazonEKSWorkerNodePolicy | 448 |
| Utilizzo di questa politica | 448 |
| Dettagli della politica | 448 |
| Versione della politica | 448 |
| Documento di policy JSON | 448 |
| Ulteriori informazioni | 449 |
| AmazonElastiCacheFullAccess | 449 |
| Utilizzo di questa politica | 449 |
| Dettagli della politica | 449 |
| Versione della politica | 450 |
| Documento di policy JSON | 450 |
| Ulteriori informazioni | 453 |
| AmazonElastiCacheReadOnlyAccess | 453 |
| Utilizzo di questa politica | 453 |
| Dettagli della politica | 454 |
| Versione della politica | 454 |
| Documento di policy JSON | 454 |
| Ulteriori informazioni | 454 |

| | |
|--|-----|
| AmazonElasticContainerRegistryPublicFullAccess | 455 |
| Utilizzo di questa politica | 455 |
| Dettagli della politica | 455 |
| Versione della politica | 455 |
| Documento di policy JSON | 455 |
| Ulteriori informazioni | 456 |
| AmazonElasticContainerRegistryPublicPowerUser | 456 |
| Utilizzo di questa politica | 456 |
| Dettagli della politica | 456 |
| Versione della politica | 456 |
| Documento di policy JSON | 457 |
| Ulteriori informazioni | 457 |
| AmazonElasticContainerRegistryPublicReadOnly | 457 |
| Utilizzo di questa politica | 458 |
| Dettagli della politica | 458 |
| Versione della politica | 458 |
| Documento di policy JSON | 458 |
| Ulteriori informazioni | 459 |
| AmazonElasticFileSystemClientFullAccess | 459 |
| Utilizzo di questa politica | 459 |
| Dettagli della politica | 459 |
| Versione della politica | 459 |
| Documento di policy JSON | 460 |
| Ulteriori informazioni | 460 |
| AmazonElasticFileSystemClientReadOnlyAccess | 460 |
| Utilizzo di questa politica | 460 |
| Dettagli della politica | 460 |
| Versione della politica | 461 |
| Documento di policy JSON | 461 |
| Ulteriori informazioni | 461 |
| AmazonElasticFileSystemClientReadWriteAccess | 461 |
| Utilizzo di questa politica | 462 |
| Dettagli della politica | 462 |
| Versione della politica | 462 |
| Documento di policy JSON | 462 |
| Ulteriori informazioni | 463 |

| | |
|--|-----|
| AmazonElasticFileSystemFullAccess | 463 |
| Utilizzo di questa politica | 463 |
| Dettagli della politica | 463 |
| Versione della politica | 463 |
| Documento di policy JSON | 463 |
| Ulteriori informazioni | 465 |
| AmazonElasticFileSystemReadOnlyAccess | 465 |
| Utilizzo di questa politica | 465 |
| Dettagli della politica | 466 |
| Versione della politica | 466 |
| Documento di policy JSON | 466 |
| Ulteriori informazioni | 467 |
| AmazonElasticFileSystemServiceRolePolicy | 467 |
| Utilizzo di questa politica | 467 |
| Dettagli della politica | 467 |
| Versione della politica | 468 |
| Documento di policy JSON | 468 |
| Ulteriori informazioni | 470 |
| AmazonElasticFileSystemsUtils | 470 |
| Utilizzo di questa politica | 470 |
| Dettagli della politica | 470 |
| Versione della politica | 470 |
| Documento di policy JSON | 471 |
| Ulteriori informazioni | 472 |
| AmazonElasticMapReduceEditorsRole | 473 |
| Utilizzo di questa politica | 473 |
| Dettagli della politica | 473 |
| Versione della politica | 473 |
| Documento di policy JSON | 473 |
| Ulteriori informazioni | 474 |
| AmazonElasticMapReduceforAutoScalingRole | 475 |
| Utilizzo di questa politica | 475 |
| Dettagli della politica | 475 |
| Versione della politica | 475 |
| Documento di policy JSON | 475 |
| Ulteriori informazioni | 476 |

| | |
|--|-----|
| AmazonElasticMapReduceforEC2Role | 476 |
| Utilizzo di questa politica | 476 |
| Dettagli della politica | 476 |
| Versione della politica | 476 |
| Documento di policy JSON | 477 |
| Ulteriori informazioni | 478 |
| AmazonElasticMapReduceFullAccess | 478 |
| Utilizzo di questa politica | 478 |
| Dettagli della politica | 478 |
| Versione della politica | 479 |
| Documento di policy JSON | 479 |
| Ulteriori informazioni | 480 |
| AmazonElasticMapReducePlacementGroupPolicy | 481 |
| Utilizzo di questa politica | 481 |
| Dettagli della politica | 481 |
| Versione della politica | 481 |
| Documento di policy JSON | 481 |
| Ulteriori informazioni | 482 |
| AmazonElasticMapReduceReadOnlyAccess | 482 |
| Utilizzo di questa politica | 482 |
| Dettagli della politica | 482 |
| Versione della politica | 483 |
| Documento di policy JSON | 483 |
| Ulteriori informazioni | 483 |
| AmazonElasticMapReduceRole | 484 |
| Utilizzo di questa politica | 484 |
| Dettagli della politica | 484 |
| Versione della politica | 484 |
| Documento di policy JSON | 484 |
| Ulteriori informazioni | 486 |
| AmazonElasticsearchServiceRolePolicy | 487 |
| Utilizzo di questa politica | 487 |
| Dettagli della politica | 487 |
| Versione della politica | 487 |
| Documento di policy JSON | 487 |
| Ulteriori informazioni | 490 |

| | |
|--|-----|
| AmazonElasticTranscoder_FullAccess | 490 |
| Utilizzo di questa politica | 490 |
| Dettagli della politica | 490 |
| Versione della politica | 491 |
| Documento di policy JSON | 491 |
| Ulteriori informazioni | 492 |
| AmazonElasticTranscoder_JobsSubmitter | 492 |
| Utilizzo di questa politica | 492 |
| Dettagli della politica | 492 |
| Versione della politica | 492 |
| Documento di policy JSON | 493 |
| Ulteriori informazioni | 493 |
| AmazonElasticTranscoder_ReadOnlyAccess | 493 |
| Utilizzo di questa politica | 493 |
| Dettagli della politica | 494 |
| Versione della politica | 494 |
| Documento di policy JSON | 494 |
| Ulteriori informazioni | 494 |
| AmazonElasticTranscoderRole | 495 |
| Utilizzo di questa politica | 495 |
| Dettagli della politica | 495 |
| Versione della politica | 495 |
| Documento di policy JSON | 495 |
| Ulteriori informazioni | 496 |
| AmazonEMRCleanupPolicy | 496 |
| Utilizzo di questa politica | 496 |
| Dettagli della politica | 497 |
| Versione della politica | 497 |
| Documento di policy JSON | 497 |
| Ulteriori informazioni | 498 |
| AmazonEMRContainersServiceRolePolicy | 498 |
| Utilizzo di questa politica | 498 |
| Dettagli della politica | 498 |
| Versione della politica | 498 |
| Documento di policy JSON | 499 |
| Ulteriori informazioni | 500 |

| | |
|--|-----|
| AmazonEMRFullAccessPolicy_v2 | 500 |
| Utilizzo di questa politica | 500 |
| Dettagli della politica | 500 |
| Versione della politica | 500 |
| Documento di policy JSON | 501 |
| Ulteriori informazioni | 504 |
| AmazonEMRReadOnlyAccessPolicy_v2 | 504 |
| Utilizzo di questa politica | 504 |
| Dettagli della politica | 504 |
| Versione della politica | 505 |
| Documento di policy JSON | 505 |
| Ulteriori informazioni | 506 |
| AmazonEMRServerlessServiceRolePolicy | 506 |
| Utilizzo di questa politica | 506 |
| Dettagli della politica | 506 |
| Versione della politica | 506 |
| Documento di policy JSON | 507 |
| Ulteriori informazioni | 508 |
| AmazonEMRServicePolicy_v2 | 508 |
| Utilizzo di questa politica | 508 |
| Dettagli della politica | 508 |
| Versione della politica | 508 |
| Documento di policy JSON | 508 |
| Ulteriori informazioni | 516 |
| AmazonESCognitoAccess | 516 |
| Utilizzo di questa politica | 516 |
| Dettagli della politica | 516 |
| Versione della politica | 517 |
| Documento di policy JSON | 517 |
| Ulteriori informazioni | 518 |
| AmazonESFullAccess | 518 |
| Utilizzo di questa politica | 518 |
| Dettagli della politica | 518 |
| Versione della politica | 518 |
| Documento di policy JSON | 519 |
| Ulteriori informazioni | 519 |

| | |
|---|-----|
| AmazonESReadOnlyAccess | 519 |
| Utilizzo di questa politica | 519 |
| Dettagli della politica | 519 |
| Versione della politica | 520 |
| Documento di policy JSON | 520 |
| Ulteriori informazioni | 520 |
| AmazonEventBridgeApiDestinationsServiceRolePolicy | 521 |
| Utilizzo di questa politica | 521 |
| Dettagli della politica | 521 |
| Versione della politica | 521 |
| Documento di policy JSON | 521 |
| Ulteriori informazioni | 522 |
| AmazonEventBridgeFullAccess | 522 |
| Utilizzo di questa politica | 522 |
| Dettagli della politica | 522 |
| Versione della politica | 522 |
| Documento di policy JSON | 523 |
| Ulteriori informazioni | 525 |
| AmazonEventBridgePipesFullAccess | 525 |
| Utilizzo di questa politica | 525 |
| Dettagli della politica | 525 |
| Versione della politica | 525 |
| Documento di policy JSON | 525 |
| Ulteriori informazioni | 526 |
| AmazonEventBridgePipesOperatorAccess | 526 |
| Utilizzo di questa politica | 526 |
| Dettagli della politica | 527 |
| Versione della politica | 527 |
| Documento di policy JSON | 527 |
| Ulteriori informazioni | 527 |
| AmazonEventBridgePipesReadOnlyAccess | 528 |
| Utilizzo di questa politica | 528 |
| Dettagli della politica | 528 |
| Versione della politica | 528 |
| Documento di policy JSON | 528 |
| Ulteriori informazioni | 529 |

| | |
|---|-----|
| AmazonEventBridgeReadOnlyAccess | 529 |
| Utilizzo di questa politica | 529 |
| Dettagli della politica | 529 |
| Versione della politica | 529 |
| Documento di policy JSON | 530 |
| Ulteriori informazioni | 531 |
| AmazonEventBridgeSchedulerFullAccess | 531 |
| Utilizzo di questa politica | 531 |
| Dettagli della politica | 531 |
| Versione della politica | 532 |
| Documento di policy JSON | 532 |
| Ulteriori informazioni | 532 |
| AmazonEventBridgeSchedulerReadOnlyAccess | 533 |
| Utilizzo di questa politica | 533 |
| Dettagli della politica | 533 |
| Versione della politica | 533 |
| Documento di policy JSON | 533 |
| Ulteriori informazioni | 534 |
| AmazonEventBridgeSchemasFullAccess | 534 |
| Utilizzo di questa politica | 534 |
| Dettagli della politica | 534 |
| Versione della politica | 534 |
| Documento di policy JSON | 535 |
| Ulteriori informazioni | 535 |
| AmazonEventBridgeSchemasReadOnlyAccess | 536 |
| Utilizzo di questa politica | 536 |
| Dettagli della politica | 536 |
| Versione della politica | 536 |
| Documento di policy JSON | 536 |
| Ulteriori informazioni | 537 |
| AmazonEventBridgeSchemasServiceRolePolicy | 537 |
| Utilizzo di questa politica | 537 |
| Dettagli della politica | 537 |
| Versione della politica | 538 |
| Documento di policy JSON | 538 |
| Ulteriori informazioni | 538 |

| | |
|---|-----|
| AmazonFISServiceRolePolicy | 539 |
| Utilizzo di questa politica | 539 |
| Dettagli della politica | 539 |
| Versione della politica | 539 |
| Documento di policy JSON | 539 |
| Ulteriori informazioni | 541 |
| AmazonForecastFullAccess | 541 |
| Utilizzo di questa politica | 541 |
| Dettagli della politica | 541 |
| Versione della politica | 541 |
| Documento di policy JSON | 542 |
| Ulteriori informazioni | 542 |
| AmazonFraudDetectorFullAccessPolicy | 543 |
| Utilizzo di questa politica | 543 |
| Dettagli della politica | 543 |
| Versione della politica | 543 |
| Documento di policy JSON | 543 |
| Ulteriori informazioni | 544 |
| AmazonFreeRTOSFullAccess | 545 |
| Utilizzo di questa politica | 545 |
| Dettagli della politica | 545 |
| Versione della politica | 545 |
| Documento di policy JSON | 545 |
| Ulteriori informazioni | 546 |
| AmazonFreeRTOSOTAUpdate | 546 |
| Utilizzo di questa politica | 546 |
| Dettagli della politica | 546 |
| Versione della politica | 546 |
| Documento di policy JSON | 546 |
| Ulteriori informazioni | 548 |
| AmazonFSxConsoleFullAccess | 548 |
| Utilizzo di questa politica | 548 |
| Dettagli della politica | 548 |
| Versione della politica | 548 |
| Documento di policy JSON | 549 |
| Ulteriori informazioni | 552 |

| | |
|--------------------------------------|-----|
| AmazonFSxConsoleReadOnlyAccess | 552 |
| Utilizzo di questa politica | 552 |
| Dettagli della politica | 552 |
| Versione della politica | 553 |
| Documento di policy JSON | 553 |
| Ulteriori informazioni | 554 |
| AmazonFSxFullAccess | 554 |
| Utilizzo di questa politica | 554 |
| Dettagli della politica | 554 |
| Versione della politica | 554 |
| Documento di policy JSON | 554 |
| Ulteriori informazioni | 558 |
| AmazonFSxReadOnlyAccess | 559 |
| Utilizzo di questa politica | 559 |
| Dettagli della politica | 559 |
| Versione della politica | 559 |
| Documento di policy JSON | 559 |
| Ulteriori informazioni | 560 |
| AmazonFSxServiceRolePolicy | 560 |
| Utilizzo di questa politica | 560 |
| Dettagli della politica | 560 |
| Versione della politica | 560 |
| Documento di policy JSON | 561 |
| Ulteriori informazioni | 563 |
| AmazonGlacierFullAccess | 563 |
| Utilizzo di questa politica | 564 |
| Dettagli della politica | 564 |
| Versione della politica | 564 |
| Documento di policy JSON | 564 |
| Ulteriori informazioni | 564 |
| AmazonGlacierReadOnlyAccess | 565 |
| Utilizzo di questa politica | 565 |
| Dettagli della politica | 565 |
| Versione della politica | 565 |
| Documento di policy JSON | 565 |
| Ulteriori informazioni | 566 |

| | |
|---|-----|
| AmazonGrafanaAthenaAccess | 566 |
| Utilizzo di questa politica | 566 |
| Dettagli della politica | 566 |
| Versione della politica | 567 |
| Documento di policy JSON | 567 |
| Ulteriori informazioni | 568 |
| AmazonGrafanaCloudWatchAccess | 569 |
| Utilizzo di questa politica | 569 |
| Dettagli della politica | 569 |
| Versione della politica | 569 |
| Documento di policy JSON | 569 |
| Ulteriori informazioni | 571 |
| AmazonGrafanaRedshiftAccess | 571 |
| Utilizzo di questa politica | 571 |
| Dettagli della politica | 571 |
| Versione della politica | 571 |
| Documento di policy JSON | 572 |
| Ulteriori informazioni | 573 |
| AmazonGrafanaServiceLinkedRolePolicy | 573 |
| Utilizzo di questa politica | 573 |
| Dettagli della politica | 573 |
| Versione della politica | 574 |
| Documento di policy JSON | 574 |
| Ulteriori informazioni | 575 |
| AmazonGuardDutyFullAccess | 575 |
| Utilizzo di questa politica | 575 |
| Dettagli della politica | 575 |
| Versione della politica | 576 |
| Documento di policy JSON | 576 |
| Ulteriori informazioni | 577 |
| AmazonGuardDutyMalwareProtectionServiceRolePolicy | 577 |
| Utilizzo di questa politica | 578 |
| Dettagli della politica | 578 |
| Versione della politica | 578 |
| Documento di policy JSON | 578 |
| Ulteriori informazioni | 583 |

| | |
|--|-----|
| AmazonGuardDutyReadOnlyAccess | 583 |
| Utilizzo di questa politica | 583 |
| Dettagli della politica | 583 |
| Versione della politica | 583 |
| Documento di policy JSON | 583 |
| Ulteriori informazioni | 584 |
| AmazonGuardDutyServiceRolePolicy | 584 |
| Utilizzo di questa politica | 585 |
| Dettagli della politica | 585 |
| Versione della politica | 585 |
| Documento di policy JSON | 585 |
| Ulteriori informazioni | 591 |
| AmazonHealthLakeFullAccess | 591 |
| Utilizzo di questa politica | 591 |
| Dettagli della politica | 591 |
| Versione della politica | 592 |
| Documento di policy JSON | 592 |
| Ulteriori informazioni | 593 |
| AmazonHealthLakeReadOnlyAccess | 593 |
| Utilizzo di questa politica | 593 |
| Dettagli della politica | 593 |
| Versione della politica | 593 |
| Documento di policy JSON | 593 |
| Ulteriori informazioni | 594 |
| AmazonHoneycodeFullAccess | 594 |
| Utilizzo di questa politica | 594 |
| Dettagli della politica | 594 |
| Versione della politica | 595 |
| Documento di policy JSON | 595 |
| Ulteriori informazioni | 595 |
| AmazonHoneycodeReadOnlyAccess | 595 |
| Utilizzo di questa politica | 596 |
| Dettagli della politica | 596 |
| Versione della politica | 596 |
| Documento di policy JSON | 596 |
| Ulteriori informazioni | 597 |

| | |
|--|-----|
| AmazonHoneycodeServiceRolePolicy | 597 |
| Utilizzo di questa politica | 597 |
| Dettagli della politica | 597 |
| Versione della politica | 597 |
| Documento di policy JSON | 598 |
| Ulteriori informazioni | 598 |
| AmazonHoneycodeTeamAssociationFullAccess | 598 |
| Utilizzo di questa politica | 598 |
| Dettagli della politica | 598 |
| Versione della politica | 599 |
| Documento di policy JSON | 599 |
| Ulteriori informazioni | 599 |
| AmazonHoneycodeTeamAssociationReadOnlyAccess | 599 |
| Utilizzo di questa politica | 600 |
| Dettagli della politica | 600 |
| Versione della politica | 600 |
| Documento di policy JSON | 600 |
| Ulteriori informazioni | 600 |
| AmazonHoneycodeWorkbookFullAccess | 601 |
| Utilizzo di questa politica | 601 |
| Dettagli della politica | 601 |
| Versione della politica | 601 |
| Documento di policy JSON | 601 |
| Ulteriori informazioni | 602 |
| AmazonHoneycodeWorkbookReadOnlyAccess | 602 |
| Utilizzo di questa politica | 602 |
| Dettagli della politica | 602 |
| Versione della politica | 603 |
| Documento di policy JSON | 603 |
| Ulteriori informazioni | 603 |
| AmazonInspector2AgentlessServiceRolePolicy | 604 |
| Utilizzo di questa politica | 604 |
| Dettagli della politica | 604 |
| Versione della politica | 604 |
| Documento di policy JSON | 604 |
| Ulteriori informazioni | 608 |

| | |
|---|-----|
| AmazonInspector2FullAccess | 608 |
| Utilizzo di questa politica | 608 |
| Dettagli della politica | 608 |
| Versione della politica | 608 |
| Documento di policy JSON | 609 |
| Ulteriori informazioni | 610 |
| AmazonInspector2ManagedCisPolicy | 610 |
| Utilizzo di questa politica | 610 |
| Dettagli della politica | 610 |
| Versione della politica | 611 |
| Documento di policy JSON | 611 |
| Ulteriori informazioni | 611 |
| AmazonInspector2ReadOnlyAccess | 611 |
| Utilizzo di questa politica | 612 |
| Dettagli della politica | 612 |
| Versione della politica | 612 |
| Documento di policy JSON | 612 |
| Ulteriori informazioni | 613 |
| AmazonInspector2ServiceRolePolicy | 613 |
| Utilizzo di questa politica | 613 |
| Dettagli della politica | 613 |
| Versione della politica | 613 |
| Documento di policy JSON | 614 |
| Ulteriori informazioni | 620 |
| AmazonInspectorFullAccess | 620 |
| Utilizzo di questa politica | 620 |
| Dettagli della politica | 620 |
| Versione della politica | 621 |
| Documento di policy JSON | 621 |
| Ulteriori informazioni | 622 |
| AmazonInspectorReadOnlyAccess | 622 |
| Utilizzo di questa politica | 622 |
| Dettagli della politica | 622 |
| Versione della politica | 622 |
| Documento di policy JSON | 623 |
| Ulteriori informazioni | 623 |

| | |
|--|-----|
| AmazonInspectorServiceRolePolicy | 623 |
| Utilizzo di questa politica | 624 |
| Dettagli della politica | 624 |
| Versione della politica | 624 |
| Documento di policy JSON | 624 |
| Ulteriori informazioni | 625 |
| AmazonKendraFullAccess | 626 |
| Utilizzo di questa politica | 626 |
| Dettagli della politica | 626 |
| Versione della politica | 626 |
| Documento di policy JSON | 626 |
| Ulteriori informazioni | 628 |
| AmazonKendraReadOnlyAccess | 628 |
| Utilizzo di questa politica | 628 |
| Dettagli della politica | 628 |
| Versione della politica | 629 |
| Documento di policy JSON | 629 |
| Ulteriori informazioni | 629 |
| AmazonKeyspacesFullAccess | 630 |
| Utilizzo di questa politica | 630 |
| Dettagli della politica | 630 |
| Versione della politica | 630 |
| Documento di policy JSON | 630 |
| Ulteriori informazioni | 632 |
| AmazonKeyspacesReadOnlyAccess | 632 |
| Utilizzo di questa politica | 632 |
| Dettagli della politica | 632 |
| Versione della politica | 633 |
| Documento di policy JSON | 633 |
| Ulteriori informazioni | 634 |
| AmazonKeyspacesReadOnlyAccess_v2 | 634 |
| Utilizzo di questa politica | 634 |
| Dettagli della politica | 634 |
| Versione della politica | 634 |
| Documento di policy JSON | 634 |
| Ulteriori informazioni | 635 |

| | |
|---|-----|
| AmazonKinesisAnalyticsFullAccess | 636 |
| Utilizzo di questa politica | 636 |
| Dettagli della politica | 636 |
| Versione della politica | 636 |
| Documento di policy JSON | 636 |
| Ulteriori informazioni | 638 |
| AmazonKinesisAnalyticsReadOnly | 638 |
| Utilizzo di questa politica | 638 |
| Dettagli della politica | 638 |
| Versione della politica | 638 |
| Documento di policy JSON | 639 |
| Ulteriori informazioni | 640 |
| AmazonKinesisFirehoseFullAccess | 640 |
| Utilizzo di questa politica | 640 |
| Dettagli della politica | 640 |
| Versione della politica | 640 |
| Documento di policy JSON | 641 |
| Ulteriori informazioni | 641 |
| AmazonKinesisFirehoseReadOnlyAccess | 641 |
| Utilizzo di questa politica | 641 |
| Dettagli della politica | 641 |
| Versione della politica | 642 |
| Documento di policy JSON | 642 |
| Ulteriori informazioni | 642 |
| AmazonKinesisFullAccess | 642 |
| Utilizzo di questa politica | 643 |
| Dettagli della politica | 643 |
| Versione della politica | 643 |
| Documento di policy JSON | 643 |
| Ulteriori informazioni | 643 |
| AmazonKinesisReadOnlyAccess | 644 |
| Utilizzo di questa politica | 644 |
| Dettagli della politica | 644 |
| Versione della politica | 644 |
| Documento di policy JSON | 644 |
| Ulteriori informazioni | 645 |

| | |
|---|-----|
| AmazonKinesisVideoStreamsFullAccess | 645 |
| Utilizzo di questa politica | 645 |
| Dettagli della politica | 645 |
| Versione della politica | 645 |
| Documento di policy JSON | 646 |
| Ulteriori informazioni | 646 |
| AmazonKinesisVideoStreamsReadOnlyAccess | 646 |
| Utilizzo di questa politica | 646 |
| Dettagli della politica | 646 |
| Versione della politica | 647 |
| Documento di policy JSON | 647 |
| Ulteriori informazioni | 647 |
| AmazonLaunchWizard_Fullaccess | 647 |
| Utilizzo di questa politica | 648 |
| Dettagli della politica | 648 |
| Versione della politica | 648 |
| Documento di policy JSON | 648 |
| Ulteriori informazioni | 662 |
| AmazonLaunchWizardFullAccessV2 | 662 |
| Utilizzo di questa politica | 663 |
| Dettagli della politica | 663 |
| Versione della politica | 663 |
| Documento di policy JSON | 663 |
| Ulteriori informazioni | 680 |
| AmazonLexChannelsAccess | 680 |
| Utilizzo di questa politica | 680 |
| Dettagli della politica | 680 |
| Versione della politica | 680 |
| Documento di policy JSON | 680 |
| Ulteriori informazioni | 681 |
| AmazonLexFullAccess | 681 |
| Utilizzo di questa politica | 681 |
| Dettagli della politica | 681 |
| Versione della politica | 681 |
| Documento di policy JSON | 682 |
| Ulteriori informazioni | 687 |

| | |
|--|-----|
| AmazonLexReadOnly | 687 |
| Utilizzo di questa politica | 687 |
| Dettagli della politica | 688 |
| Versione della politica | 688 |
| Documento di policy JSON | 688 |
| Ulteriori informazioni | 689 |
| AmazonLexReplicationPolicy | 690 |
| Utilizzo di questa politica | 690 |
| Dettagli della politica | 690 |
| Versione della politica | 690 |
| Documento di policy JSON | 690 |
| Ulteriori informazioni | 693 |
| AmazonLexRunBotsOnly | 693 |
| Utilizzo di questa politica | 693 |
| Dettagli della politica | 693 |
| Versione della politica | 693 |
| Documento di policy JSON | 693 |
| Ulteriori informazioni | 694 |
| AmazonLexV2BotPolicy | 694 |
| Utilizzo di questa politica | 694 |
| Dettagli della politica | 694 |
| Versione della politica | 695 |
| Documento di policy JSON | 695 |
| Ulteriori informazioni | 695 |
| AmazonLookoutEquipmentFullAccess | 695 |
| Utilizzo di questa politica | 695 |
| Dettagli della politica | 696 |
| Versione della politica | 696 |
| Documento di policy JSON | 696 |
| Ulteriori informazioni | 697 |
| AmazonLookoutEquipmentReadOnlyAccess | 697 |
| Utilizzo di questa politica | 697 |
| Dettagli della politica | 698 |
| Versione della politica | 698 |
| Documento di policy JSON | 698 |
| Ulteriori informazioni | 698 |

| | |
|--|-----|
| AmazonLookoutMetricsFullAccess | 699 |
| Utilizzo di questa politica | 699 |
| Dettagli della politica | 699 |
| Versione della politica | 699 |
| Documento di policy JSON | 699 |
| Ulteriori informazioni | 700 |
| AmazonLookoutMetricsReadOnlyAccess | 700 |
| Utilizzo di questa politica | 700 |
| Dettagli della politica | 700 |
| Versione della politica | 701 |
| Documento di policy JSON | 701 |
| Ulteriori informazioni | 701 |
| AmazonLookoutVisionConsoleFullAccess | 702 |
| Utilizzo di questa politica | 702 |
| Dettagli della politica | 702 |
| Versione della politica | 702 |
| Documento di policy JSON | 702 |
| Ulteriori informazioni | 704 |
| AmazonLookoutVisionConsoleReadOnlyAccess | 705 |
| Utilizzo di questa politica | 705 |
| Dettagli della politica | 705 |
| Versione della politica | 705 |
| Documento di policy JSON | 705 |
| Ulteriori informazioni | 707 |
| AmazonLookoutVisionFullAccess | 707 |
| Utilizzo di questa politica | 707 |
| Dettagli della politica | 707 |
| Versione della politica | 707 |
| Documento di policy JSON | 707 |
| Ulteriori informazioni | 708 |
| AmazonLookoutVisionReadOnlyAccess | 708 |
| Utilizzo di questa politica | 708 |
| Dettagli della politica | 708 |
| Versione della politica | 709 |
| Documento di policy JSON | 709 |
| Ulteriori informazioni | 709 |

| | |
|---|-----|
| AmazonMachineLearningBatchPredictionsAccess | 710 |
| Utilizzo di questa politica | 710 |
| Dettagli della politica | 710 |
| Versione della politica | 710 |
| Documento di policy JSON | 710 |
| Ulteriori informazioni | 711 |
| AmazonMachineLearningCreateOnlyAccess | 711 |
| Utilizzo di questa politica | 711 |
| Dettagli della politica | 711 |
| Versione della politica | 711 |
| Documento di policy JSON | 712 |
| Ulteriori informazioni | 712 |
| AmazonMachineLearningFullAccess | 712 |
| Utilizzo di questa politica | 712 |
| Dettagli della politica | 712 |
| Versione della politica | 713 |
| Documento di policy JSON | 713 |
| Ulteriori informazioni | 713 |
| AmazonMachineLearningManageRealTimeEndpointOnlyAccess | 713 |
| Utilizzo di questa politica | 714 |
| Dettagli della politica | 714 |
| Versione della politica | 714 |
| Documento di policy JSON | 714 |
| Ulteriori informazioni | 715 |
| AmazonMachineLearningReadOnlyAccess | 715 |
| Utilizzo di questa politica | 715 |
| Dettagli della politica | 715 |
| Versione della politica | 715 |
| Documento di policy JSON | 715 |
| Ulteriori informazioni | 716 |
| AmazonMachineLearningRealTimePredictionOnlyAccess | 716 |
| Utilizzo di questa politica | 716 |
| Dettagli della politica | 716 |
| Versione della politica | 717 |
| Documento di policy JSON | 717 |
| Ulteriori informazioni | 717 |

| | |
|--|-----|
| AmazonMachineLearningRoleforRedshiftDataSourceV3 | 717 |
| Utilizzo di questa politica | 718 |
| Dettagli della politica | 718 |
| Versione della politica | 718 |
| Documento di policy JSON | 718 |
| Ulteriori informazioni | 719 |
| AmazonMacieFullAccess | 719 |
| Utilizzo di questa politica | 719 |
| Dettagli della politica | 719 |
| Versione della politica | 720 |
| Documento di policy JSON | 720 |
| Ulteriori informazioni | 721 |
| AmazonMacieHandshakeRole | 721 |
| Utilizzo di questa politica | 721 |
| Dettagli della politica | 721 |
| Versione della politica | 721 |
| Documento di policy JSON | 721 |
| Ulteriori informazioni | 722 |
| AmazonMacieReadOnlyAccess | 722 |
| Utilizzo di questa politica | 722 |
| Dettagli della politica | 722 |
| Versione della politica | 723 |
| Documento di policy JSON | 723 |
| Ulteriori informazioni | 723 |
| AmazonMacieServiceRole | 723 |
| Utilizzo di questa politica | 724 |
| Dettagli della politica | 724 |
| Versione della politica | 724 |
| Documento di policy JSON | 724 |
| Ulteriori informazioni | 724 |
| AmazonMacieServiceRolePolicy | 725 |
| Utilizzo di questa politica | 725 |
| Dettagli della politica | 725 |
| Versione della politica | 725 |
| Documento di policy JSON | 725 |
| Ulteriori informazioni | 727 |

| | |
|--|-----|
| AmazonManagedBlockchainConsoleFullAccess | 727 |
| Utilizzo di questa politica | 727 |
| Dettagli della politica | 727 |
| Versione della politica | 727 |
| Documento di policy JSON | 727 |
| Ulteriori informazioni | 728 |
| AmazonManagedBlockchainFullAccess | 728 |
| Utilizzo di questa politica | 728 |
| Dettagli della politica | 728 |
| Versione della politica | 729 |
| Documento di policy JSON | 729 |
| Ulteriori informazioni | 729 |
| AmazonManagedBlockchainReadOnlyAccess | 729 |
| Utilizzo di questa politica | 730 |
| Dettagli della politica | 730 |
| Versione della politica | 730 |
| Documento di policy JSON | 730 |
| Ulteriori informazioni | 731 |
| AmazonManagedBlockchainServiceRolePolicy | 731 |
| Utilizzo di questa politica | 731 |
| Dettagli della politica | 731 |
| Versione della politica | 731 |
| Documento di policy JSON | 732 |
| Ulteriori informazioni | 732 |
| AmazonMCSFullAccess | 732 |
| Utilizzo di questa politica | 732 |
| Dettagli della politica | 733 |
| Versione della politica | 733 |
| Documento di policy JSON | 733 |
| Ulteriori informazioni | 734 |
| AmazonMCSReadOnlyAccess | 734 |
| Utilizzo di questa politica | 735 |
| Dettagli della politica | 735 |
| Versione della politica | 735 |
| Documento di policy JSON | 735 |
| Ulteriori informazioni | 736 |

| | |
|--|-----|
| AmazonMechanicalTurkFullAccess | 736 |
| Utilizzo di questa politica | 736 |
| Dettagli della politica | 736 |
| Versione della politica | 736 |
| Documento di policy JSON | 737 |
| Ulteriori informazioni | 737 |
| AmazonMechanicalTurkReadOnly | 737 |
| Utilizzo di questa politica | 737 |
| Dettagli della politica | 737 |
| Versione della politica | 738 |
| Documento di policy JSON | 738 |
| Ulteriori informazioni | 738 |
| AmazonMemoryDBFullAccess | 738 |
| Utilizzo di questa politica | 739 |
| Dettagli della politica | 739 |
| Versione della politica | 739 |
| Documento di policy JSON | 739 |
| Ulteriori informazioni | 740 |
| AmazonMemoryDBReadOnlyAccess | 740 |
| Utilizzo di questa politica | 740 |
| Dettagli della politica | 740 |
| Versione della politica | 740 |
| Documento di policy JSON | 741 |
| Ulteriori informazioni | 741 |
| AmazonMobileAnalyticsFinancialReportAccess | 741 |
| Utilizzo di questa politica | 741 |
| Dettagli della politica | 741 |
| Versione della politica | 742 |
| Documento di policy JSON | 742 |
| Ulteriori informazioni | 742 |
| AmazonMobileAnalyticsFullAccess | 742 |
| Utilizzo di questa politica | 743 |
| Dettagli della politica | 743 |
| Versione della politica | 743 |
| Documento di policy JSON | 743 |
| Ulteriori informazioni | 743 |

| | |
|--|-----|
| AmazonMobileAnalyticsNon-financialReportAccess | 744 |
| Utilizzo di questa politica | 744 |
| Dettagli della politica | 744 |
| Versione della politica | 744 |
| Documento di policy JSON | 744 |
| Ulteriori informazioni | 745 |
| AmazonMobileAnalyticsWriteOnlyAccess | 745 |
| Utilizzo di questa politica | 745 |
| Dettagli della politica | 745 |
| Versione della politica | 745 |
| Documento di policy JSON | 746 |
| Ulteriori informazioni | 746 |
| AmazonMonitronFullAccess | 746 |
| Utilizzo di questa politica | 746 |
| Dettagli della politica | 746 |
| Versione della politica | 747 |
| Documento di policy JSON | 747 |
| Ulteriori informazioni | 749 |
| AmazonMQApiFullAccess | 749 |
| Utilizzo di questa politica | 749 |
| Dettagli della politica | 749 |
| Versione della politica | 749 |
| Documento di policy JSON | 749 |
| Ulteriori informazioni | 750 |
| AmazonMQApiReadOnlyAccess | 751 |
| Utilizzo di questa politica | 751 |
| Dettagli della politica | 751 |
| Versione della politica | 751 |
| Documento di policy JSON | 751 |
| Ulteriori informazioni | 752 |
| AmazonMQFullAccess | 752 |
| Utilizzo di questa politica | 752 |
| Dettagli della politica | 752 |
| Versione della politica | 752 |
| Documento di policy JSON | 753 |
| Ulteriori informazioni | 754 |

| | |
|--------------------------------------|-----|
| AmazonMQReadOnlyAccess | 754 |
| Utilizzo di questa politica | 754 |
| Dettagli della politica | 754 |
| Versione della politica | 754 |
| Documento di policy JSON | 755 |
| Ulteriori informazioni | 755 |
| AmazonMQServiceRolePolicy | 755 |
| Utilizzo di questa politica | 756 |
| Dettagli della politica | 756 |
| Versione della politica | 756 |
| Documento di policy JSON | 756 |
| Ulteriori informazioni | 758 |
| AmazonMSKConnectReadOnlyAccess | 758 |
| Utilizzo di questa politica | 758 |
| Dettagli della politica | 758 |
| Versione della politica | 758 |
| Documento di policy JSON | 759 |
| Ulteriori informazioni | 760 |
| AmazonMSKFullAccess | 760 |
| Utilizzo di questa politica | 760 |
| Dettagli della politica | 760 |
| Versione della politica | 760 |
| Documento di policy JSON | 761 |
| Ulteriori informazioni | 763 |
| AmazonMSKReadOnlyAccess | 764 |
| Utilizzo di questa politica | 764 |
| Dettagli della politica | 764 |
| Versione della politica | 764 |
| Documento di policy JSON | 764 |
| Ulteriori informazioni | 765 |
| AmazonMWAAServiceRolePolicy | 765 |
| Utilizzo di questa politica | 765 |
| Dettagli della politica | 765 |
| Versione della politica | 765 |
| Documento di policy JSON | 766 |
| Ulteriori informazioni | 768 |

| | |
|--|-----|
| AmazonNimbleStudio-LaunchProfileWorker | 768 |
| Utilizzo di questa politica | 768 |
| Dettagli della politica | 768 |
| Versione della politica | 768 |
| Documento di policy JSON | 769 |
| Ulteriori informazioni | 769 |
| AmazonNimbleStudio-StudioAdmin | 770 |
| Utilizzo di questa politica | 770 |
| Dettagli della politica | 770 |
| Versione della politica | 770 |
| Documento di policy JSON | 770 |
| Ulteriori informazioni | 772 |
| AmazonNimbleStudio-StudioUser | 772 |
| Utilizzo di questa politica | 772 |
| Dettagli della politica | 773 |
| Versione della politica | 773 |
| Documento di policy JSON | 773 |
| Ulteriori informazioni | 775 |
| AmazonOmicsFullAccess | 775 |
| Utilizzo di questa politica | 775 |
| Dettagli della politica | 775 |
| Versione della politica | 776 |
| Documento di policy JSON | 776 |
| Ulteriori informazioni | 777 |
| AmazonOmicsReadOnlyAccess | 777 |
| Utilizzo di questa politica | 777 |
| Dettagli della politica | 777 |
| Versione della politica | 777 |
| Documento di policy JSON | 778 |
| Ulteriori informazioni | 778 |
| AmazonOneEnterpriseFullAccess | 778 |
| Utilizzo di questa politica | 778 |
| Dettagli della politica | 779 |
| Versione della politica | 779 |
| Documento di policy JSON | 779 |
| Ulteriori informazioni | 779 |

| | |
|---|-----|
| AmazonOneEnterpriseInstallerAccess | 780 |
| Utilizzo di questa politica | 780 |
| Dettagli della politica | 780 |
| Versione della politica | 780 |
| Documento di policy JSON | 780 |
| Ulteriori informazioni | 781 |
| AmazonOneEnterpriseReadOnlyAccess | 781 |
| Utilizzo di questa politica | 781 |
| Dettagli della politica | 781 |
| Versione della politica | 781 |
| Documento di policy JSON | 782 |
| Ulteriori informazioni | 782 |
| AmazonOpenSearchDashboardsServiceRolePolicy | 782 |
| Utilizzo di questa politica | 782 |
| Dettagli della politica | 783 |
| Versione della politica | 783 |
| Documento di policy JSON | 783 |
| Ulteriori informazioni | 783 |
| AmazonOpenSearchDirectQueryGlueCreateAccess | 784 |
| Utilizzo di questa politica | 784 |
| Dettagli della politica | 784 |
| Versione della politica | 784 |
| Documento di policy JSON | 784 |
| Ulteriori informazioni | 785 |
| AmazonOpenSearchIngestionFullAccess | 785 |
| Utilizzo di questa politica | 785 |
| Dettagli della politica | 785 |
| Versione della politica | 785 |
| Documento di policy JSON | 786 |
| Ulteriori informazioni | 786 |
| AmazonOpenSearchIngestionReadOnlyAccess | 787 |
| Utilizzo di questa politica | 787 |
| Dettagli della politica | 787 |
| Versione della politica | 787 |
| Documento di policy JSON | 787 |
| Ulteriori informazioni | 788 |

| | |
|---|-----|
| AmazonOpenSearchIngestionServiceRolePolicy | 788 |
| Utilizzo di questa politica | 788 |
| Dettagli della politica | 788 |
| Versione della politica | 789 |
| Documento di policy JSON | 789 |
| Ulteriori informazioni | 791 |
| AmazonOpenSearchServerlessServiceRolePolicy | 791 |
| Utilizzo di questa politica | 791 |
| Dettagli della politica | 791 |
| Versione della politica | 791 |
| Documento di policy JSON | 791 |
| Ulteriori informazioni | 792 |
| AmazonOpenSearchServiceCognitoAccess | 792 |
| Utilizzo di questa politica | 792 |
| Dettagli della politica | 792 |
| Versione della politica | 792 |
| Documento di policy JSON | 793 |
| Ulteriori informazioni | 794 |
| AmazonOpenSearchServiceFullAccess | 794 |
| Utilizzo di questa politica | 794 |
| Dettagli della politica | 794 |
| Versione della politica | 794 |
| Documento di policy JSON | 795 |
| Ulteriori informazioni | 795 |
| AmazonOpenSearchServiceReadOnlyAccess | 795 |
| Utilizzo di questa politica | 795 |
| Dettagli della politica | 796 |
| Versione della politica | 796 |
| Documento di policy JSON | 796 |
| Ulteriori informazioni | 796 |
| AmazonOpenSearchServiceRolePolicy | 797 |
| Utilizzo di questa politica | 797 |
| Dettagli della politica | 797 |
| Versione della politica | 797 |
| Documento di policy JSON | 797 |
| Ulteriori informazioni | 802 |

| | |
|---|-----|
| AmazonPersonalizeFullAccess | 802 |
| Utilizzo di questa politica | 802 |
| Dettagli della politica | 802 |
| Versione della politica | 802 |
| Documento di policy JSON | 803 |
| Ulteriori informazioni | 804 |
| AmazonPollyFullAccess | 804 |
| Utilizzo di questa politica | 804 |
| Dettagli della politica | 804 |
| Versione della politica | 804 |
| Documento di policy JSON | 805 |
| Ulteriori informazioni | 805 |
| AmazonPollyReadOnlyAccess | 805 |
| Utilizzo di questa politica | 805 |
| Dettagli della politica | 806 |
| Versione della politica | 806 |
| Documento di policy JSON | 806 |
| Ulteriori informazioni | 806 |
| AmazonPrometheusConsoleFullAccess | 807 |
| Utilizzo di questa politica | 807 |
| Dettagli della politica | 807 |
| Versione della politica | 807 |
| Documento di policy JSON | 807 |
| Ulteriori informazioni | 808 |
| AmazonPrometheusFullAccess | 809 |
| Utilizzo di questa politica | 809 |
| Dettagli della politica | 809 |
| Versione della politica | 809 |
| Documento di policy JSON | 809 |
| Ulteriori informazioni | 810 |
| AmazonPrometheusQueryAccess | 810 |
| Utilizzo di questa politica | 811 |
| Dettagli della politica | 811 |
| Versione della politica | 811 |
| Documento di policy JSON | 811 |
| Ulteriori informazioni | 812 |

| | |
|--|-----|
| AmazonPrometheusRemoteWriteAccess | 812 |
| Utilizzo di questa politica | 812 |
| Dettagli della politica | 812 |
| Versione della politica | 812 |
| Documento di policy JSON | 812 |
| Ulteriori informazioni | 813 |
| AmazonPrometheusScraperServiceRolePolicy | 813 |
| Utilizzo di questa politica | 813 |
| Dettagli della politica | 813 |
| Versione della politica | 814 |
| Documento di policy JSON | 814 |
| Ulteriori informazioni | 816 |
| AmazonQFullAccess | 816 |
| Utilizzo di questa politica | 816 |
| Dettagli della politica | 816 |
| Versione della politica | 817 |
| Documento di policy JSON | 817 |
| Ulteriori informazioni | 817 |
| AmazonQLDBConsoleFullAccess | 818 |
| Utilizzo di questa politica | 818 |
| Dettagli della politica | 818 |
| Versione della politica | 818 |
| Documento di policy JSON | 818 |
| Ulteriori informazioni | 820 |
| AmazonQLDBFullAccess | 820 |
| Utilizzo di questa politica | 820 |
| Dettagli della politica | 820 |
| Versione della politica | 821 |
| Documento di policy JSON | 821 |
| Ulteriori informazioni | 822 |
| AmazonQLDBReadOnly | 822 |
| Utilizzo di questa politica | 822 |
| Dettagli della politica | 823 |
| Versione della politica | 823 |
| Documento di policy JSON | 823 |
| Ulteriori informazioni | 824 |

| | |
|--|-----|
| AmazonRDSBetaServiceRolePolicy | 824 |
| Utilizzo di questa politica | 824 |
| Dettagli della politica | 824 |
| Versione della politica | 824 |
| Documento di policy JSON | 824 |
| Ulteriori informazioni | 828 |
| AmazonRDSCustomInstanceProfileRolePolicy | 828 |
| Utilizzo di questa politica | 828 |
| Dettagli della politica | 828 |
| Versione della politica | 828 |
| Documento di policy JSON | 828 |
| Ulteriori informazioni | 836 |
| AmazonRDSCustomPreviewServiceRolePolicy | 836 |
| Utilizzo di questa politica | 836 |
| Dettagli della politica | 836 |
| Versione della politica | 836 |
| Documento di policy JSON | 836 |
| Ulteriori informazioni | 852 |
| AmazonRDSCustomServiceRolePolicy | 852 |
| Utilizzo di questa politica | 852 |
| Dettagli della politica | 852 |
| Versione della politica | 853 |
| Documento di policy JSON | 853 |
| Ulteriori informazioni | 870 |
| AmazonRDSDDataFullAccess | 870 |
| Utilizzo di questa politica | 870 |
| Dettagli della politica | 871 |
| Versione della politica | 871 |
| Documento di policy JSON | 871 |
| Ulteriori informazioni | 872 |
| AmazonRDSDirectoryServiceAccess | 872 |
| Utilizzo di questa politica | 872 |
| Dettagli della politica | 873 |
| Versione della politica | 873 |
| Documento di policy JSON | 873 |
| Ulteriori informazioni | 873 |

| | |
|--|-----|
| AmazonRDSEnhancedMonitoringRole | 874 |
| Utilizzo di questa politica | 874 |
| Dettagli della politica | 874 |
| Versione della politica | 874 |
| Documento di policy JSON | 874 |
| Ulteriori informazioni | 875 |
| AmazonRDSFullAccess | 875 |
| Utilizzo di questa politica | 875 |
| Dettagli della politica | 875 |
| Versione della politica | 876 |
| Documento di policy JSON | 876 |
| Ulteriori informazioni | 878 |
| AmazonRDSPerformanceInsightsFullAccess | 878 |
| Utilizzo di questa politica | 878 |
| Dettagli della politica | 878 |
| Versione della politica | 879 |
| Documento di policy JSON | 879 |
| Ulteriori informazioni | 880 |
| AmazonRDSPerformanceInsightsReadOnly | 880 |
| Utilizzo di questa politica | 881 |
| Dettagli della politica | 881 |
| Versione della politica | 881 |
| Documento di policy JSON | 881 |
| Ulteriori informazioni | 883 |
| AmazonRDSPreviewServiceRolePolicy | 883 |
| Utilizzo di questa politica | 883 |
| Dettagli della politica | 883 |
| Versione della politica | 883 |
| Documento di policy JSON | 884 |
| Ulteriori informazioni | 887 |
| AmazonRDSReadOnlyAccess | 887 |
| Utilizzo di questa politica | 887 |
| Dettagli della politica | 887 |
| Versione della politica | 887 |
| Documento di policy JSON | 888 |
| Ulteriori informazioni | 889 |

| | |
|---|-----|
| AmazonRDSServiceRolePolicy | 889 |
| Utilizzo di questa politica | 889 |
| Dettagli della politica | 889 |
| Versione della politica | 889 |
| Documento di policy JSON | 890 |
| Ulteriori informazioni | 894 |
| AmazonRedshiftAllCommandsFullAccess | 894 |
| Utilizzo di questa politica | 894 |
| Dettagli della politica | 894 |
| Versione della politica | 894 |
| Documento di policy JSON | 894 |
| Ulteriori informazioni | 900 |
| AmazonRedshiftDataFullAccess | 900 |
| Utilizzo di questa politica | 900 |
| Dettagli della politica | 900 |
| Versione della politica | 900 |
| Documento di policy JSON | 901 |
| Ulteriori informazioni | 903 |
| AmazonRedshiftFullAccess | 903 |
| Utilizzo di questa politica | 903 |
| Dettagli della politica | 903 |
| Versione della politica | 903 |
| Documento di policy JSON | 903 |
| Ulteriori informazioni | 905 |
| AmazonRedshiftQueryEditor | 906 |
| Utilizzo di questa politica | 906 |
| Dettagli della politica | 906 |
| Versione della politica | 906 |
| Documento di policy JSON | 906 |
| Ulteriori informazioni | 908 |
| AmazonRedshiftQueryEditorV2FullAccess | 908 |
| Utilizzo di questa politica | 909 |
| Dettagli della politica | 909 |
| Versione della politica | 909 |
| Documento di policy JSON | 909 |
| Ulteriori informazioni | 910 |

| | |
|---|-----|
| AmazonRedshiftQueryEditorV2NoSharing | 911 |
| Utilizzo di questa politica | 911 |
| Dettagli della politica | 911 |
| Versione della politica | 911 |
| Documento di policy JSON | 911 |
| Ulteriori informazioni | 915 |
| AmazonRedshiftQueryEditorV2ReadSharing | 915 |
| Utilizzo di questa politica | 915 |
| Dettagli della politica | 915 |
| Versione della politica | 916 |
| Documento di policy JSON | 916 |
| Ulteriori informazioni | 921 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing | 921 |
| Utilizzo di questa politica | 921 |
| Dettagli della politica | 921 |
| Versione della politica | 921 |
| Documento di policy JSON | 922 |
| Ulteriori informazioni | 927 |
| AmazonRedshiftReadOnlyAccess | 927 |
| Utilizzo di questa politica | 927 |
| Dettagli della politica | 927 |
| Versione della politica | 927 |
| Documento di policy JSON | 927 |
| Ulteriori informazioni | 928 |
| AmazonRedshiftServiceLinkedRolePolicy | 928 |
| Utilizzo di questa politica | 929 |
| Dettagli della politica | 929 |
| Versione della politica | 929 |
| Documento di policy JSON | 929 |
| Ulteriori informazioni | 934 |
| AmazonRekognitionCustomLabelsFullAccess | 935 |
| Utilizzo di questa politica | 935 |
| Dettagli della politica | 935 |
| Versione della politica | 935 |
| Documento di policy JSON | 935 |
| Ulteriori informazioni | 936 |

| | |
|---|-----|
| AmazonRekognitionFullAccess | 937 |
| Utilizzo di questa politica | 937 |
| Dettagli della politica | 937 |
| Versione della politica | 937 |
| Documento di policy JSON | 937 |
| Ulteriori informazioni | 938 |
| AmazonRekognitionReadOnlyAccess | 938 |
| Utilizzo di questa politica | 938 |
| Dettagli della politica | 938 |
| Versione della politica | 938 |
| Documento di policy JSON | 939 |
| Ulteriori informazioni | 940 |
| AmazonRekognitionServiceRole | 940 |
| Utilizzo di questa politica | 940 |
| Dettagli della politica | 940 |
| Versione della politica | 940 |
| Documento di policy JSON | 941 |
| Ulteriori informazioni | 941 |
| AmazonRoute53AutoNamingFullAccess | 942 |
| Utilizzo di questa politica | 942 |
| Dettagli della politica | 942 |
| Versione della politica | 942 |
| Documento di policy JSON | 942 |
| Ulteriori informazioni | 943 |
| AmazonRoute53AutoNamingReadOnlyAccess | 943 |
| Utilizzo di questa politica | 943 |
| Dettagli della politica | 943 |
| Versione della politica | 944 |
| Documento di policy JSON | 944 |
| Ulteriori informazioni | 944 |
| AmazonRoute53AutoNamingRegistrantAccess | 944 |
| Utilizzo di questa politica | 945 |
| Dettagli della politica | 945 |
| Versione della politica | 945 |
| Documento di policy JSON | 945 |
| Ulteriori informazioni | 946 |

| | |
|---|-----|
| AmazonRoute53DomainsFullAccess | 946 |
| Utilizzo di questa politica | 946 |
| Dettagli della politica | 946 |
| Versione della politica | 946 |
| Documento di policy JSON | 947 |
| Ulteriori informazioni | 947 |
| AmazonRoute53DomainsReadOnlyAccess | 947 |
| Utilizzo di questa politica | 947 |
| Dettagli della politica | 947 |
| Versione della politica | 948 |
| Documento di policy JSON | 948 |
| Ulteriori informazioni | 948 |
| AmazonRoute53FullAccess | 949 |
| Utilizzo di questa politica | 949 |
| Dettagli della politica | 949 |
| Versione della politica | 949 |
| Documento di policy JSON | 949 |
| Ulteriori informazioni | 950 |
| AmazonRoute53ProfilesFullAccess | 950 |
| Utilizzo di questa politica | 950 |
| Dettagli della politica | 950 |
| Versione della politica | 951 |
| Documento di policy JSON | 951 |
| Ulteriori informazioni | 952 |
| AmazonRoute53ProfilesReadOnlyAccess | 952 |
| Utilizzo di questa politica | 952 |
| Dettagli della politica | 952 |
| Versione della politica | 953 |
| Documento di policy JSON | 953 |
| Ulteriori informazioni | 953 |
| AmazonRoute53ReadOnlyAccess | 954 |
| Utilizzo di questa politica | 954 |
| Dettagli della politica | 954 |
| Versione della politica | 954 |
| Documento di policy JSON | 954 |
| Ulteriori informazioni | 955 |

| | |
|--|-----|
| AmazonRoute53RecoveryClusterFullAccess | 955 |
| Utilizzo di questa politica | 955 |
| Dettagli della politica | 955 |
| Versione della politica | 955 |
| Documento di policy JSON | 956 |
| Ulteriori informazioni | 956 |
| AmazonRoute53RecoveryClusterReadOnlyAccess | 956 |
| Utilizzo di questa politica | 956 |
| Dettagli della politica | 956 |
| Versione della politica | 957 |
| Documento di policy JSON | 957 |
| Ulteriori informazioni | 957 |
| AmazonRoute53RecoveryControlConfigFullAccess | 957 |
| Utilizzo di questa politica | 958 |
| Dettagli della politica | 958 |
| Versione della politica | 958 |
| Documento di policy JSON | 958 |
| Ulteriori informazioni | 959 |
| AmazonRoute53RecoveryControlConfigReadOnlyAccess | 959 |
| Utilizzo di questa politica | 959 |
| Dettagli della politica | 959 |
| Versione della politica | 959 |
| Documento di policy JSON | 959 |
| Ulteriori informazioni | 960 |
| AmazonRoute53RecoveryReadinessFullAccess | 960 |
| Utilizzo di questa politica | 960 |
| Dettagli della politica | 961 |
| Versione della politica | 961 |
| Documento di policy JSON | 961 |
| Ulteriori informazioni | 961 |
| AmazonRoute53RecoveryReadinessReadOnlyAccess | 962 |
| Utilizzo di questa politica | 962 |
| Dettagli della politica | 962 |
| Versione della politica | 962 |
| Documento di policy JSON | 962 |
| Ulteriori informazioni | 963 |

| | |
|---|-----|
| AmazonRoute53ResolverFullAccess | 963 |
| Utilizzo di questa politica | 963 |
| Dettagli della politica | 964 |
| Versione della politica | 964 |
| Documento di policy JSON | 964 |
| Ulteriori informazioni | 965 |
| AmazonRoute53ResolverReadOnlyAccess | 965 |
| Utilizzo di questa politica | 965 |
| Dettagli della politica | 965 |
| Versione della politica | 965 |
| Documento di policy JSON | 965 |
| Ulteriori informazioni | 966 |
| AmazonS3FullAccess | 966 |
| Utilizzo di questa politica | 966 |
| Dettagli della politica | 966 |
| Versione della politica | 967 |
| Documento di policy JSON | 967 |
| Ulteriori informazioni | 967 |
| AmazonS3ObjectLambdaExecutionRolePolicy | 967 |
| Utilizzo di questa politica | 968 |
| Dettagli della politica | 968 |
| Versione della politica | 968 |
| Documento di policy JSON | 968 |
| Ulteriori informazioni | 969 |
| AmazonS3OutpostsFullAccess | 969 |
| Utilizzo di questa politica | 969 |
| Dettagli della politica | 969 |
| Versione della politica | 969 |
| Documento di policy JSON | 969 |
| Ulteriori informazioni | 970 |
| AmazonS3OutpostsReadOnlyAccess | 971 |
| Utilizzo di questa politica | 971 |
| Dettagli della politica | 971 |
| Versione della politica | 971 |
| Documento di policy JSON | 971 |
| Ulteriori informazioni | 972 |

| | |
|--|------|
| AmazonS3ReadOnlyAccess | 973 |
| Utilizzo di questa politica | 973 |
| Dettagli della politica | 973 |
| Versione della politica | 973 |
| Documento di policy JSON | 973 |
| Ulteriori informazioni | 974 |
| AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy | 974 |
| Utilizzo di questa politica | 974 |
| Dettagli della politica | 974 |
| Versione della politica | 975 |
| Documento di policy JSON | 975 |
| Ulteriori informazioni | 985 |
| AmazonSageMakerCanvasAIServicesAccess | 985 |
| Utilizzo di questa politica | 985 |
| Dettagli della politica | 985 |
| Versione della politica | 985 |
| Documento di policy JSON | 986 |
| Ulteriori informazioni | 989 |
| AmazonSageMakerCanvasBedrockAccess | 989 |
| Utilizzo di questa politica | 989 |
| Dettagli della politica | 989 |
| Versione della politica | 989 |
| Documento di policy JSON | 990 |
| Ulteriori informazioni | 990 |
| AmazonSageMakerCanvasDataPrepFullAccess | 991 |
| Utilizzo di questa politica | 991 |
| Dettagli della politica | 991 |
| Versione della politica | 991 |
| Documento di policy JSON | 991 |
| Ulteriori informazioni | 998 |
| AmazonSageMakerCanvasDirectDeployAccess | 999 |
| Utilizzo di questa politica | 999 |
| Dettagli della politica | 999 |
| Versione della politica | 999 |
| Documento di policy JSON | 999 |
| Ulteriori informazioni | 1000 |

| | |
|--|------|
| AmazonSageMakerCanvasForecastAccess | 1000 |
| Utilizzo di questa politica | 1000 |
| Dettagli della politica | 1001 |
| Versione della politica | 1001 |
| Documento di policy JSON | 1001 |
| Ulteriori informazioni | 1002 |
| AmazonSageMakerCanvasFullAccess | 1002 |
| Utilizzo di questa politica | 1002 |
| Dettagli della politica | 1002 |
| Versione della politica | 1002 |
| Documento di policy JSON | 1003 |
| Ulteriori informazioni | 1011 |
| AmazonSageMakerClusterInstanceRolePolicy | 1011 |
| Utilizzo di questa politica | 1011 |
| Dettagli della politica | 1011 |
| Versione della politica | 1011 |
| Documento di policy JSON | 1011 |
| Ulteriori informazioni | 1013 |
| AmazonSageMakerCoreServiceRolePolicy | 1013 |
| Utilizzo di questa politica | 1014 |
| Dettagli della politica | 1014 |
| Versione della politica | 1014 |
| Documento di policy JSON | 1014 |
| Ulteriori informazioni | 1015 |
| AmazonSageMakerEdgeDeviceFleetPolicy | 1015 |
| Utilizzo di questa politica | 1015 |
| Dettagli della politica | 1015 |
| Versione della politica | 1016 |
| Documento di policy JSON | 1016 |
| Ulteriori informazioni | 1018 |
| AmazonSageMakerFeatureStoreAccess | 1018 |
| Utilizzo di questa politica | 1018 |
| Dettagli della politica | 1018 |
| Versione della politica | 1018 |
| Documento di policy JSON | 1019 |
| Ulteriori informazioni | 1020 |

| | |
|---|------|
| AmazonSageMakerFullAccess | 1020 |
| Utilizzo di questa politica | 1020 |
| Dettagli della politica | 1020 |
| Versione della politica | 1020 |
| Documento di policy JSON | 1020 |
| Ulteriori informazioni | 1036 |
| AmazonSageMakerGeospatialExecutionRole | 1037 |
| Utilizzo di questa politica | 1037 |
| Dettagli della politica | 1037 |
| Versione della politica | 1037 |
| Documento di policy JSON | 1037 |
| Ulteriori informazioni | 1038 |
| AmazonSageMakerGeospatialFullAccess | 1038 |
| Utilizzo di questa politica | 1038 |
| Dettagli della politica | 1039 |
| Versione della politica | 1039 |
| Documento di policy JSON | 1039 |
| Ulteriori informazioni | 1040 |
| AmazonSageMakerGroundTruthExecution | 1040 |
| Utilizzo di questa politica | 1040 |
| Dettagli della politica | 1040 |
| Versione della politica | 1040 |
| Documento di policy JSON | 1041 |
| Ulteriori informazioni | 1044 |
| AmazonSageMakerMechanicalTurkAccess | 1044 |
| Utilizzo di questa politica | 1044 |
| Dettagli della politica | 1044 |
| Versione della politica | 1045 |
| Documento di policy JSON | 1045 |
| Ulteriori informazioni | 1045 |
| AmazonSageMakerModelGovernanceUseAccess | 1046 |
| Utilizzo di questa politica | 1046 |
| Dettagli della politica | 1046 |
| Versione della politica | 1046 |
| Documento di policy JSON | 1046 |
| Ulteriori informazioni | 1048 |

| | |
|---|------|
| AmazonSageMakerModelRegistryFullAccess | 1048 |
| Utilizzo di questa politica | 1048 |
| Dettagli della politica | 1049 |
| Versione della politica | 1049 |
| Documento di policy JSON | 1049 |
| Ulteriori informazioni | 1053 |
| AmazonSageMakerNotebooksServiceRolePolicy | 1053 |
| Utilizzo di questa politica | 1053 |
| Dettagli della politica | 1053 |
| Versione della politica | 1053 |
| Documento di policy JSON | 1053 |
| Ulteriori informazioni | 1057 |
| AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy | 1058 |
| Utilizzo di questa politica | 1058 |
| Dettagli della politica | 1058 |
| Versione della politica | 1058 |
| Documento di policy JSON | 1058 |
| Ulteriori informazioni | 1059 |
| AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy | 1059 |
| Utilizzo di questa politica | 1060 |
| Dettagli della politica | 1060 |
| Versione della politica | 1060 |
| Documento di policy JSON | 1060 |
| Ulteriori informazioni | 1064 |
| AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy | 1064 |
| Utilizzo di questa politica | 1064 |
| Dettagli della politica | 1064 |
| Versione della politica | 1064 |
| Documento di policy JSON | 1065 |
| Ulteriori informazioni | 1065 |
| AmazonSageMakerPipelinesIntegrations | 1065 |
| Utilizzo di questa politica | 1066 |
| Dettagli della politica | 1066 |
| Versione della politica | 1066 |
| Documento di policy JSON | 1066 |
| Ulteriori informazioni | 1068 |

| | |
|--|------|
| AmazonSageMakerReadOnly | 1068 |
| Utilizzo di questa politica | 1068 |
| Dettagli della politica | 1068 |
| Versione della politica | 1069 |
| Documento di policy JSON | 1069 |
| Ulteriori informazioni | 1070 |
| AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy | 1070 |
| Utilizzo di questa politica | 1070 |
| Dettagli della politica | 1070 |
| Versione della politica | 1071 |
| Documento di policy JSON | 1071 |
| Ulteriori informazioni | 1072 |
| AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy | 1072 |
| Utilizzo di questa politica | 1072 |
| Dettagli della politica | 1072 |
| Versione della politica | 1072 |
| Documento di policy JSON | 1073 |
| Ulteriori informazioni | 1079 |
| AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy | 1080 |
| Utilizzo di questa politica | 1080 |
| Dettagli della politica | 1080 |
| Versione della politica | 1080 |
| Documento di policy JSON | 1080 |
| Ulteriori informazioni | 1090 |
| AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy | 1091 |
| Utilizzo di questa politica | 1091 |
| Dettagli della politica | 1091 |
| Versione della politica | 1091 |
| Documento di policy JSON | 1091 |
| Ulteriori informazioni | 1094 |
| AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy | 1094 |
| Utilizzo di questa politica | 1095 |
| Dettagli della politica | 1095 |
| Versione della politica | 1095 |
| Documento di policy JSON | 1095 |
| Ulteriori informazioni | 1095 |

| | |
|--|------|
| AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy | 1096 |
| Utilizzo di questa politica | 1096 |
| Dettagli della politica | 1096 |
| Versione della politica | 1096 |
| Documento di policy JSON | 1096 |
| Ulteriori informazioni | 1097 |
| AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy | 1097 |
| Utilizzo di questa politica | 1097 |
| Dettagli della politica | 1097 |
| Versione della politica | 1098 |
| Documento di policy JSON | 1098 |
| Ulteriori informazioni | 1100 |
| AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy | 1100 |
| Utilizzo di questa politica | 1100 |
| Dettagli della politica | 1101 |
| Versione della politica | 1101 |
| Documento di policy JSON | 1101 |
| Ulteriori informazioni | 1111 |
| AmazonSecurityLakeAdministrator | 1111 |
| Utilizzo di questa politica | 1111 |
| Dettagli della politica | 1111 |
| Versione della politica | 1112 |
| Documento di policy JSON | 1112 |
| Ulteriori informazioni | 1123 |
| AmazonSecurityLakeMetastoreManager | 1123 |
| Utilizzo di questa politica | 1123 |
| Dettagli della politica | 1123 |
| Versione della politica | 1124 |
| Documento di policy JSON | 1124 |
| Ulteriori informazioni | 1126 |
| AmazonSecurityLakePermissionsBoundary | 1126 |
| Utilizzo di questa politica | 1126 |
| Dettagli della politica | 1127 |
| Versione della politica | 1127 |
| Documento di policy JSON | 1127 |
| Ulteriori informazioni | 1130 |

| | |
|-----------------------------------|------|
| AmazonSESEFullAccess | 1130 |
| Utilizzo di questa politica | 1130 |
| Dettagli della politica | 1131 |
| Versione della politica | 1131 |
| Documento di policy JSON | 1131 |
| Ulteriori informazioni | 1131 |
| AmazonSESReadOnlyAccess | 1132 |
| Utilizzo di questa politica | 1132 |
| Dettagli della politica | 1132 |
| Versione della politica | 1132 |
| Documento di policy JSON | 1132 |
| Ulteriori informazioni | 1133 |
| AmazonSESServiceRolePolicy | 1133 |
| Utilizzo di questa politica | 1133 |
| Dettagli della politica | 1133 |
| Versione della politica | 1133 |
| Documento di policy JSON | 1134 |
| Ulteriori informazioni | 1134 |
| AmazonSNSFullAccess | 1134 |
| Utilizzo di questa politica | 1134 |
| Dettagli della politica | 1134 |
| Versione della politica | 1135 |
| Documento di policy JSON | 1135 |
| Ulteriori informazioni | 1135 |
| AmazonSNSReadOnlyAccess | 1135 |
| Utilizzo di questa politica | 1136 |
| Dettagli della politica | 1136 |
| Versione della politica | 1136 |
| Documento di policy JSON | 1136 |
| Ulteriori informazioni | 1136 |
| AmazonSNSRole | 1137 |
| Utilizzo di questa politica | 1137 |
| Dettagli della politica | 1137 |
| Versione della politica | 1137 |
| Documento di policy JSON | 1137 |
| Ulteriori informazioni | 1138 |

| | |
|---|------|
| AmazonSQSFullAccess | 1138 |
| Utilizzo di questa politica | 1138 |
| Dettagli della politica | 1138 |
| Versione della politica | 1139 |
| Documento di policy JSON | 1139 |
| Ulteriori informazioni | 1139 |
| AmazonSQSReadOnlyAccess | 1139 |
| Utilizzo di questa politica | 1139 |
| Dettagli della politica | 1140 |
| Versione della politica | 1140 |
| Documento di policy JSON | 1140 |
| Ulteriori informazioni | 1140 |
| AmazonSSMAutomationApproverAccess | 1141 |
| Utilizzo di questa politica | 1141 |
| Dettagli della politica | 1141 |
| Versione della politica | 1141 |
| Documento di policy JSON | 1141 |
| Ulteriori informazioni | 1142 |
| AmazonSSMAutomationRole | 1142 |
| Utilizzo di questa politica | 1142 |
| Dettagli della politica | 1142 |
| Versione della politica | 1143 |
| Documento di policy JSON | 1143 |
| Ulteriori informazioni | 1144 |
| AmazonSSMDirectoryServiceAccess | 1144 |
| Utilizzo di questa politica | 1145 |
| Dettagli della politica | 1145 |
| Versione della politica | 1145 |
| Documento di policy JSON | 1145 |
| Ulteriori informazioni | 1145 |
| AmazonSSMFullAccess | 1146 |
| Utilizzo di questa politica | 1146 |
| Dettagli della politica | 1146 |
| Versione della politica | 1146 |
| Documento di policy JSON | 1146 |
| Ulteriori informazioni | 1147 |

| | |
|--|------|
| AmazonSSMMaintenanceWindowRole | 1148 |
| Utilizzo di questa politica | 1148 |
| Dettagli della politica | 1148 |
| Versione della politica | 1148 |
| Documento di policy JSON | 1148 |
| Ulteriori informazioni | 1150 |
| AmazonSSMManagedEC2InstanceDefaultPolicy | 1150 |
| Utilizzo di questa politica | 1150 |
| Dettagli della politica | 1150 |
| Versione della politica | 1150 |
| Documento di policy JSON | 1151 |
| Ulteriori informazioni | 1152 |
| AmazonSSMManagedInstanceCore | 1152 |
| Utilizzo di questa politica | 1152 |
| Dettagli della politica | 1152 |
| Versione della politica | 1152 |
| Documento di policy JSON | 1153 |
| Ulteriori informazioni | 1154 |
| AmazonSSMPatchAssociation | 1154 |
| Utilizzo di questa politica | 1154 |
| Dettagli della politica | 1154 |
| Versione della politica | 1155 |
| Documento di policy JSON | 1155 |
| Ulteriori informazioni | 1155 |
| AmazonSSMReadOnlyAccess | 1156 |
| Utilizzo di questa politica | 1156 |
| Dettagli della politica | 1156 |
| Versione della politica | 1156 |
| Documento di policy JSON | 1156 |
| Ulteriori informazioni | 1157 |
| AmazonSSMServiceRolePolicy | 1157 |
| Utilizzo di questa politica | 1157 |
| Dettagli della politica | 1157 |
| Versione della politica | 1157 |
| Documento di policy JSON | 1158 |
| Ulteriori informazioni | 1163 |

| | |
|--|------|
| AmazonSumerianFullAccess | 1163 |
| Utilizzo di questa politica | 1163 |
| Dettagli della politica | 1163 |
| Versione della politica | 1163 |
| Documento di policy JSON | 1163 |
| Ulteriori informazioni | 1164 |
| AmazonTextractFullAccess | 1164 |
| Utilizzo di questa politica | 1164 |
| Dettagli della politica | 1164 |
| Versione della politica | 1164 |
| Documento di policy JSON | 1165 |
| Ulteriori informazioni | 1165 |
| AmazonTextractServiceRole | 1165 |
| Utilizzo di questa politica | 1165 |
| Dettagli della politica | 1165 |
| Versione della politica | 1166 |
| Documento di policy JSON | 1166 |
| Ulteriori informazioni | 1166 |
| AmazonTimestreamConsoleFullAccess | 1166 |
| Utilizzo di questa politica | 1167 |
| Dettagli della politica | 1167 |
| Versione della politica | 1167 |
| Documento di policy JSON | 1167 |
| Ulteriori informazioni | 1169 |
| AmazonTimestreamFullAccess | 1169 |
| Utilizzo di questa politica | 1169 |
| Dettagli della politica | 1169 |
| Versione della politica | 1170 |
| Documento di policy JSON | 1170 |
| Ulteriori informazioni | 1171 |
| AmazonTimestreamInfluxDBFullAccess | 1171 |
| Utilizzo di questa politica | 1171 |
| Dettagli della politica | 1171 |
| Versione della politica | 1172 |
| Documento di policy JSON | 1172 |
| Ulteriori informazioni | 1174 |

| | |
|---|------|
| AmazonTimestreamInfluxDBServiceRolePolicy | 1174 |
| Utilizzo di questa politica | 1174 |
| Dettagli della politica | 1174 |
| Versione della politica | 1174 |
| Documento di policy JSON | 1175 |
| Ulteriori informazioni | 1177 |
| AmazonTimestreamReadOnlyAccess | 1177 |
| Utilizzo di questa politica | 1177 |
| Dettagli della politica | 1177 |
| Versione della politica | 1178 |
| Documento di policy JSON | 1178 |
| Ulteriori informazioni | 1179 |
| AmazonTranscribeFullAccess | 1179 |
| Utilizzo di questa politica | 1179 |
| Dettagli della politica | 1179 |
| Versione della politica | 1179 |
| Documento di policy JSON | 1179 |
| Ulteriori informazioni | 1180 |
| AmazonTranscribeReadOnlyAccess | 1180 |
| Utilizzo di questa politica | 1180 |
| Dettagli della politica | 1180 |
| Versione della politica | 1181 |
| Documento di policy JSON | 1181 |
| Ulteriori informazioni | 1181 |
| AmazonVPCCrossAccountNetworkInterfaceOperations | 1181 |
| Utilizzo di questa politica | 1182 |
| Dettagli della politica | 1182 |
| Versione della politica | 1182 |
| Documento di policy JSON | 1182 |
| Ulteriori informazioni | 1184 |
| AmazonVPCFullAccess | 1184 |
| Utilizzo di questa politica | 1184 |
| Dettagli della politica | 1184 |
| Versione della politica | 1184 |
| Documento di policy JSON | 1184 |
| Ulteriori informazioni | 1188 |

| | |
|--|------|
| AmazonVPCNetworkAccessAnalyzerFullAccessPolicy | 1188 |
| Utilizzo di questa politica | 1189 |
| Dettagli della politica | 1189 |
| Versione della politica | 1189 |
| Documento di policy JSON | 1189 |
| Ulteriori informazioni | 1192 |
| AmazonVPCReachabilityAnalyzerFullAccessPolicy | 1193 |
| Utilizzo di questa politica | 1193 |
| Dettagli della politica | 1193 |
| Versione della politica | 1193 |
| Documento di policy JSON | 1193 |
| Ulteriori informazioni | 1196 |
| AmazonVPCReachabilityAnalyzerPathComponentReadPolicy | 1197 |
| Utilizzo di questa politica | 1197 |
| Dettagli della politica | 1197 |
| Versione della politica | 1197 |
| Documento di policy JSON | 1197 |
| Ulteriori informazioni | 1198 |
| AmazonVPCReadOnlyAccess | 1198 |
| Utilizzo di questa politica | 1198 |
| Dettagli della politica | 1198 |
| Versione della politica | 1198 |
| Documento di policy JSON | 1199 |
| Ulteriori informazioni | 1200 |
| AmazonWorkDocsFullAccess | 1200 |
| Utilizzo di questa politica | 1200 |
| Dettagli della politica | 1200 |
| Versione della politica | 1201 |
| Documento di policy JSON | 1201 |
| Ulteriori informazioni | 1201 |
| AmazonWorkDocsReadOnlyAccess | 1201 |
| Utilizzo di questa politica | 1202 |
| Dettagli della politica | 1202 |
| Versione della politica | 1202 |
| Documento di policy JSON | 1202 |
| Ulteriori informazioni | 1203 |

| | |
|---|------|
| AmazonWorkMailEventsServiceRolePolicy | 1203 |
| Utilizzo di questa politica | 1203 |
| Dettagli della politica | 1203 |
| Versione della politica | 1203 |
| Documento di policy JSON | 1204 |
| Ulteriori informazioni | 1204 |
| AmazonWorkMailFullAccess | 1204 |
| Utilizzo di questa politica | 1204 |
| Dettagli della politica | 1204 |
| Versione della politica | 1205 |
| Documento di policy JSON | 1205 |
| Ulteriori informazioni | 1207 |
| AmazonWorkMailMessageFlowFullAccess | 1207 |
| Utilizzo di questa politica | 1207 |
| Dettagli della politica | 1207 |
| Versione della politica | 1207 |
| Documento di policy JSON | 1208 |
| Ulteriori informazioni | 1208 |
| AmazonWorkMailMessageFlowReadOnlyAccess | 1208 |
| Utilizzo di questa politica | 1208 |
| Dettagli della politica | 1208 |
| Versione della politica | 1209 |
| Documento di policy JSON | 1209 |
| Ulteriori informazioni | 1209 |
| AmazonWorkMailReadOnlyAccess | 1209 |
| Utilizzo di questa politica | 1210 |
| Dettagli della politica | 1210 |
| Versione della politica | 1210 |
| Documento di policy JSON | 1210 |
| Ulteriori informazioni | 1211 |
| AmazonWorkSpacesAdmin | 1211 |
| Utilizzo di questa politica | 1211 |
| Dettagli della politica | 1211 |
| Versione della politica | 1211 |
| Documento di policy JSON | 1212 |
| Ulteriori informazioni | 1212 |

| | |
|---|------|
| AmazonWorkSpacesApplicationManagerAdminAccess | 1213 |
| Utilizzo di questa politica | 1213 |
| Dettagli della politica | 1213 |
| Versione della politica | 1213 |
| Documento di policy JSON | 1213 |
| Ulteriori informazioni | 1214 |
| AmazonWorkspacesPCAAccess | 1214 |
| Utilizzo di questa politica | 1214 |
| Dettagli della politica | 1214 |
| Versione della politica | 1214 |
| Documento di policy JSON | 1215 |
| Ulteriori informazioni | 1215 |
| AmazonWorkSpacesSelfServiceAccess | 1215 |
| Utilizzo di questa politica | 1216 |
| Dettagli della politica | 1216 |
| Versione della politica | 1216 |
| Documento di policy JSON | 1216 |
| Ulteriori informazioni | 1216 |
| AmazonWorkSpacesServiceAccess | 1217 |
| Utilizzo di questa politica | 1217 |
| Dettagli della politica | 1217 |
| Versione della politica | 1217 |
| Documento di policy JSON | 1217 |
| Ulteriori informazioni | 1218 |
| AmazonWorkSpacesWebReadOnly | 1218 |
| Utilizzo di questa politica | 1218 |
| Dettagli della politica | 1218 |
| Versione della politica | 1218 |
| Documento di policy JSON | 1219 |
| Ulteriori informazioni | 1220 |
| AmazonWorkSpacesWebServiceRolePolicy | 1220 |
| Utilizzo di questa politica | 1220 |
| Dettagli della politica | 1220 |
| Versione della politica | 1220 |
| Documento di policy JSON | 1221 |
| Ulteriori informazioni | 1223 |

| | |
|--|------|
| AmazonZocaloFullAccess | 1223 |
| Utilizzo di questa politica | 1223 |
| Dettagli della politica | 1223 |
| Versione della politica | 1223 |
| Documento di policy JSON | 1224 |
| Ulteriori informazioni | 1224 |
| AmazonZocaloReadOnlyAccess | 1225 |
| Utilizzo di questa politica | 1225 |
| Dettagli della politica | 1225 |
| Versione della politica | 1225 |
| Documento di policy JSON | 1225 |
| Ulteriori informazioni | 1226 |
| AmplifyBackendDeployFullAccess | 1226 |
| Utilizzo di questa politica | 1226 |
| Dettagli della politica | 1226 |
| Versione della politica | 1226 |
| Documento di policy JSON | 1227 |
| Ulteriori informazioni | 1230 |
| APIGatewayServiceRolePolicy | 1231 |
| Utilizzo di questa politica | 1231 |
| Dettagli della politica | 1231 |
| Versione della politica | 1231 |
| Documento di policy JSON | 1231 |
| Ulteriori informazioni | 1233 |
| AppIntegrationsServiceLinkedRolePolicy | 1234 |
| Utilizzo di questa politica | 1234 |
| Dettagli della politica | 1234 |
| Versione della politica | 1234 |
| Documento di policy JSON | 1234 |
| Ulteriori informazioni | 1236 |
| ApplicationAutoScalingForAmazonAppStreamAccess | 1236 |
| Utilizzo di questa politica | 1236 |
| Dettagli della politica | 1236 |
| Versione della politica | 1236 |
| Documento di policy JSON | 1237 |
| Ulteriori informazioni | 1237 |

| | |
|--|------|
| ApplicationDiscoveryServiceContinuousExportServiceRolePolicy | 1238 |
| Utilizzo di questa politica | 1238 |
| Dettagli della politica | 1238 |
| Versione della politica | 1238 |
| Documento di policy JSON | 1238 |
| Ulteriori informazioni | 1240 |
| AppRunnerNetworkingServiceRolePolicy | 1240 |
| Utilizzo di questa politica | 1241 |
| Dettagli della politica | 1241 |
| Versione della politica | 1241 |
| Documento di policy JSON | 1241 |
| Ulteriori informazioni | 1242 |
| AppRunnerServiceRolePolicy | 1243 |
| Utilizzo di questa politica | 1243 |
| Dettagli della politica | 1243 |
| Versione della politica | 1243 |
| Documento di policy JSON | 1243 |
| Ulteriori informazioni | 1244 |
| AutoScalingConsoleFullAccess | 1244 |
| Utilizzo di questa politica | 1244 |
| Dettagli della politica | 1245 |
| Versione della politica | 1245 |
| Documento di policy JSON | 1245 |
| Ulteriori informazioni | 1247 |
| AutoScalingConsoleReadOnlyAccess | 1247 |
| Utilizzo di questa politica | 1247 |
| Dettagli della politica | 1247 |
| Versione della politica | 1247 |
| Documento di policy JSON | 1248 |
| Ulteriori informazioni | 1249 |
| AutoScalingFullAccess | 1249 |
| Utilizzo di questa politica | 1249 |
| Dettagli della politica | 1249 |
| Versione della politica | 1249 |
| Documento di policy JSON | 1249 |
| Ulteriori informazioni | 1251 |

| | |
|---|------|
| AutoScalingNotificationAccessRole | 1251 |
| Utilizzo di questa politica | 1251 |
| Dettagli della politica | 1251 |
| Versione della politica | 1251 |
| Documento di policy JSON | 1252 |
| Ulteriori informazioni | 1252 |
| AutoScalingReadOnlyAccess | 1252 |
| Utilizzo di questa politica | 1252 |
| Dettagli della politica | 1253 |
| Versione della politica | 1253 |
| Documento di policy JSON | 1253 |
| Ulteriori informazioni | 1253 |
| AutoScalingServiceRolePolicy | 1254 |
| Utilizzo di questa politica | 1254 |
| Dettagli della politica | 1254 |
| Versione della politica | 1254 |
| Documento di policy JSON | 1254 |
| Ulteriori informazioni | 1257 |
| AWS_ConfigRole | 1257 |
| Utilizzo di questa politica | 1257 |
| Dettagli della politica | 1257 |
| Versione della politica | 1258 |
| Documento di policy JSON | 1258 |
| Ulteriori informazioni | 1289 |
| AWSAccountActivityAccess | 1289 |
| Utilizzo di questa politica | 1289 |
| Dettagli della politica | 1289 |
| Versione della politica | 1289 |
| Documento di policy JSON | 1289 |
| Ulteriori informazioni | 1290 |
| AWSAccountManagementFullAccess | 1290 |
| Utilizzo di questa politica | 1290 |
| Dettagli della politica | 1291 |
| Versione della politica | 1291 |
| Documento di policy JSON | 1291 |
| Ulteriori informazioni | 1291 |

| | |
|--|------|
| AWSAccountManagementReadOnlyAccess | 1292 |
| Utilizzo di questa politica | 1292 |
| Dettagli della politica | 1292 |
| Versione della politica | 1292 |
| Documento di policy JSON | 1292 |
| Ulteriori informazioni | 1293 |
| AWSAccountUsageReportAccess | 1293 |
| Utilizzo di questa politica | 1293 |
| Dettagli della politica | 1293 |
| Versione della politica | 1293 |
| Documento di policy JSON | 1293 |
| Ulteriori informazioni | 1294 |
| AWSAgentlessDiscoveryService | 1294 |
| Utilizzo di questa politica | 1294 |
| Dettagli della politica | 1294 |
| Versione della politica | 1294 |
| Documento di policy JSON | 1295 |
| Ulteriori informazioni | 1296 |
| AWSAppFabricFullAccess | 1297 |
| Utilizzo di questa politica | 1297 |
| Dettagli della politica | 1297 |
| Versione della politica | 1297 |
| Documento di policy JSON | 1297 |
| Ulteriori informazioni | 1299 |
| AWSAppFabricReadOnlyAccess | 1299 |
| Utilizzo di questa politica | 1299 |
| Dettagli della politica | 1299 |
| Versione della politica | 1299 |
| Documento di policy JSON | 1299 |
| Ulteriori informazioni | 1300 |
| AWSAppFabricServiceRolePolicy | 1300 |
| Utilizzo di questa politica | 1300 |
| Dettagli della politica | 1301 |
| Versione della politica | 1301 |
| Documento di policy JSON | 1301 |
| Ulteriori informazioni | 1302 |

| | |
|--|------|
| AWSApplicationAutoscalingAppStreamFleetPolicy | 1302 |
| Utilizzo di questa politica | 1302 |
| Dettagli della politica | 1303 |
| Versione della politica | 1303 |
| Documento di policy JSON | 1303 |
| Ulteriori informazioni | 1304 |
| AWSApplicationAutoscalingCassandraTablePolicy | 1304 |
| Utilizzo di questa politica | 1304 |
| Dettagli della politica | 1304 |
| Versione della politica | 1304 |
| Documento di policy JSON | 1304 |
| Ulteriori informazioni | 1305 |
| AWSApplicationAutoscalingComprehendEndpointPolicy | 1305 |
| Utilizzo di questa politica | 1305 |
| Dettagli della politica | 1306 |
| Versione della politica | 1306 |
| Documento di policy JSON | 1306 |
| Ulteriori informazioni | 1307 |
| AWSApplicationAutoScalingCustomResourcePolicy | 1307 |
| Utilizzo di questa politica | 1307 |
| Dettagli della politica | 1307 |
| Versione della politica | 1307 |
| Documento di policy JSON | 1307 |
| Ulteriori informazioni | 1308 |
| AWSApplicationAutoscalingDynamoDBTablePolicy | 1308 |
| Utilizzo di questa politica | 1308 |
| Dettagli della politica | 1308 |
| Versione della politica | 1309 |
| Documento di policy JSON | 1309 |
| Ulteriori informazioni | 1309 |
| AWSApplicationAutoscalingEC2SpotFleetRequestPolicy | 1309 |
| Utilizzo di questa politica | 1310 |
| Dettagli della politica | 1310 |
| Versione della politica | 1310 |
| Documento di policy JSON | 1310 |
| Ulteriori informazioni | 1311 |

| | |
|--|------|
| AWSApplicationAutoscalingECSServicePolicy | 1311 |
| Utilizzo di questa politica | 1311 |
| Dettagli della politica | 1311 |
| Versione della politica | 1311 |
| Documento di policy JSON | 1312 |
| Ulteriori informazioni | 1312 |
| AWSApplicationAutoscalingElastiCacheRGPolicy | 1312 |
| Utilizzo di questa politica | 1312 |
| Dettagli della politica | 1313 |
| Versione della politica | 1313 |
| Documento di policy JSON | 1313 |
| Ulteriori informazioni | 1314 |
| AWSApplicationAutoscalingEMRInstanceGroupPolicy | 1314 |
| Utilizzo di questa politica | 1314 |
| Dettagli della politica | 1314 |
| Versione della politica | 1314 |
| Documento di policy JSON | 1315 |
| Ulteriori informazioni | 1315 |
| AWSApplicationAutoscalingKafkaClusterPolicy | 1315 |
| Utilizzo di questa politica | 1315 |
| Dettagli della politica | 1316 |
| Versione della politica | 1316 |
| Documento di policy JSON | 1316 |
| Ulteriori informazioni | 1317 |
| AWSApplicationAutoscalingLambdaConcurrencyPolicy | 1317 |
| Utilizzo di questa politica | 1317 |
| Dettagli della politica | 1317 |
| Versione della politica | 1317 |
| Documento di policy JSON | 1317 |
| Ulteriori informazioni | 1318 |
| AWSApplicationAutoscalingNeptuneClusterPolicy | 1318 |
| Utilizzo di questa politica | 1318 |
| Dettagli della politica | 1318 |
| Versione della politica | 1319 |
| Documento di policy JSON | 1319 |
| Ulteriori informazioni | 1320 |

| | |
|--|------|
| AWSApplicationAutoscalingRDSClusterPolicy | 1321 |
| Utilizzo di questa politica | 1321 |
| Dettagli della politica | 1321 |
| Versione della politica | 1321 |
| Documento di policy JSON | 1321 |
| Ulteriori informazioni | 1322 |
| AWSApplicationAutoscalingSageMakerEndpointPolicy | 1322 |
| Utilizzo di questa politica | 1322 |
| Dettagli della politica | 1323 |
| Versione della politica | 1323 |
| Documento di policy JSON | 1323 |
| Ulteriori informazioni | 1324 |
| AWSApplicationDiscoveryAgentAccess | 1324 |
| Utilizzo di questa politica | 1324 |
| Dettagli della politica | 1324 |
| Versione della politica | 1324 |
| Documento di policy JSON | 1325 |
| Ulteriori informazioni | 1325 |
| AWSApplicationDiscoveryAgentlessCollectorAccess | 1325 |
| Utilizzo di questa politica | 1326 |
| Dettagli della politica | 1326 |
| Versione della politica | 1326 |
| Documento di policy JSON | 1326 |
| Ulteriori informazioni | 1327 |
| AWSApplicationDiscoveryServiceFullAccess | 1327 |
| Utilizzo di questa politica | 1328 |
| Dettagli della politica | 1328 |
| Versione della politica | 1328 |
| Documento di policy JSON | 1328 |
| Ulteriori informazioni | 1329 |
| AWSApplicationMigrationAgentInstallationPolicy | 1330 |
| Utilizzo di questa politica | 1330 |
| Dettagli della politica | 1330 |
| Versione della politica | 1330 |
| Documento di policy JSON | 1330 |
| Ulteriori informazioni | 1331 |

| | |
|---|------|
| AWSApplicationMigrationAgentPolicy | 1332 |
| Utilizzo di questa politica | 1332 |
| Dettagli della politica | 1332 |
| Versione della politica | 1332 |
| Documento di policy JSON | 1332 |
| Ulteriori informazioni | 1333 |
| AWSApplicationMigrationAgentPolicy_v2 | 1333 |
| Utilizzo di questa politica | 1334 |
| Dettagli della politica | 1334 |
| Versione della politica | 1334 |
| Documento di policy JSON | 1334 |
| Ulteriori informazioni | 1335 |
| AWSApplicationMigrationConversionServerPolicy | 1335 |
| Utilizzo di questa politica | 1335 |
| Dettagli della politica | 1335 |
| Versione della politica | 1336 |
| Documento di policy JSON | 1336 |
| Ulteriori informazioni | 1336 |
| AWSApplicationMigrationEC2Access | 1337 |
| Utilizzo di questa politica | 1337 |
| Dettagli della politica | 1337 |
| Versione della politica | 1337 |
| Documento di policy JSON | 1337 |
| Ulteriori informazioni | 1345 |
| AWSApplicationMigrationFullAccess | 1345 |
| Utilizzo di questa politica | 1345 |
| Dettagli della politica | 1345 |
| Versione della politica | 1346 |
| Documento di policy JSON | 1346 |
| Ulteriori informazioni | 1352 |
| AWSApplicationMigrationMGHAccess | 1352 |
| Utilizzo di questa politica | 1352 |
| Dettagli della politica | 1352 |
| Versione della politica | 1353 |
| Documento di policy JSON | 1353 |
| Ulteriori informazioni | 1353 |

| | |
|---|------|
| AWSApplicationMigrationReadOnlyAccess | 1354 |
| Utilizzo di questa politica | 1354 |
| Dettagli della politica | 1354 |
| Versione della politica | 1354 |
| Documento di policy JSON | 1354 |
| Ulteriori informazioni | 1355 |
| AWSApplicationMigrationReplicationServerPolicy | 1356 |
| Utilizzo di questa politica | 1356 |
| Dettagli della politica | 1356 |
| Versione della politica | 1356 |
| Documento di policy JSON | 1356 |
| Ulteriori informazioni | 1358 |
| AWSApplicationMigrationServiceEc2InstancePolicy | 1358 |
| Utilizzo di questa politica | 1359 |
| Dettagli della politica | 1359 |
| Versione della politica | 1359 |
| Documento di policy JSON | 1359 |
| Ulteriori informazioni | 1360 |
| AWSApplicationMigrationServiceRolePolicy | 1360 |
| Utilizzo di questa politica | 1361 |
| Dettagli della politica | 1361 |
| Versione della politica | 1361 |
| Documento di policy JSON | 1361 |
| Ulteriori informazioni | 1368 |
| AWSApplicationMigrationSSMAccess | 1368 |
| Utilizzo di questa politica | 1368 |
| Dettagli della politica | 1369 |
| Versione della politica | 1369 |
| Documento di policy JSON | 1369 |
| Ulteriori informazioni | 1371 |
| AWSApplicationMigrationVCenterClientPolicy | 1371 |
| Utilizzo di questa politica | 1371 |
| Dettagli della politica | 1371 |
| Versione della politica | 1372 |
| Documento di policy JSON | 1372 |
| Ulteriori informazioni | 1372 |

| | |
|--|------|
| AWSAppMeshEnvoyAccess | 1373 |
| Utilizzo di questa politica | 1373 |
| Dettagli della politica | 1373 |
| Versione della politica | 1373 |
| Documento di policy JSON | 1373 |
| Ulteriori informazioni | 1374 |
| AWSAppMeshFullAccess | 1374 |
| Utilizzo di questa politica | 1374 |
| Dettagli della politica | 1374 |
| Versione della politica | 1374 |
| Documento di policy JSON | 1375 |
| Ulteriori informazioni | 1376 |
| AWSAppMeshPreviewEnvoyAccess | 1376 |
| Utilizzo di questa politica | 1376 |
| Dettagli della politica | 1376 |
| Versione della politica | 1377 |
| Documento di policy JSON | 1377 |
| Ulteriori informazioni | 1377 |
| AWSAppMeshPreviewServiceRolePolicy | 1377 |
| Utilizzo di questa politica | 1378 |
| Dettagli della politica | 1378 |
| Versione della politica | 1378 |
| Documento di policy JSON | 1378 |
| Ulteriori informazioni | 1379 |
| AWSAppMeshReadOnly | 1379 |
| Utilizzo di questa politica | 1379 |
| Dettagli della politica | 1379 |
| Versione della politica | 1379 |
| Documento di policy JSON | 1379 |
| Ulteriori informazioni | 1380 |
| AWSAppMeshServiceRolePolicy | 1381 |
| Utilizzo di questa politica | 1381 |
| Dettagli della politica | 1381 |
| Versione della politica | 1381 |
| Documento di policy JSON | 1381 |
| Ulteriori informazioni | 1382 |

| | |
|---|------|
| AWSAppRunnerFullAccess | 1382 |
| Utilizzo di questa politica | 1382 |
| Dettagli della politica | 1382 |
| Versione della politica | 1383 |
| Documento di policy JSON | 1383 |
| Ulteriori informazioni | 1384 |
| AWSAppRunnerReadOnlyAccess | 1384 |
| Utilizzo di questa politica | 1384 |
| Dettagli della politica | 1384 |
| Versione della politica | 1384 |
| Documento di policy JSON | 1384 |
| Ulteriori informazioni | 1385 |
| AWSAppRunnerServicePolicyForECRAccess | 1385 |
| Utilizzo di questa politica | 1385 |
| Dettagli della politica | 1385 |
| Versione della politica | 1386 |
| Documento di policy JSON | 1386 |
| Ulteriori informazioni | 1386 |
| AWSAppSyncAdministrator | 1386 |
| Utilizzo di questa politica | 1387 |
| Dettagli della politica | 1387 |
| Versione della politica | 1387 |
| Documento di policy JSON | 1387 |
| Ulteriori informazioni | 1388 |
| AWSAppSyncInvokeFullAccess | 1388 |
| Utilizzo di questa politica | 1389 |
| Dettagli della politica | 1389 |
| Versione della politica | 1389 |
| Documento di policy JSON | 1389 |
| Ulteriori informazioni | 1390 |
| AWSAppSyncPushToCloudWatchLogs | 1390 |
| Utilizzo di questa politica | 1390 |
| Dettagli della politica | 1390 |
| Versione della politica | 1390 |
| Documento di policy JSON | 1390 |
| Ulteriori informazioni | 1391 |

| | |
|--|------|
| AWSAppSyncSchemaAuthor | 1391 |
| Utilizzo di questa politica | 1391 |
| Dettagli della politica | 1391 |
| Versione della politica | 1391 |
| Documento di policy JSON | 1392 |
| Ulteriori informazioni | 1393 |
| AWSAppSyncServiceRolePolicy | 1393 |
| Utilizzo di questa politica | 1393 |
| Dettagli della politica | 1393 |
| Versione della politica | 1393 |
| Documento di policy JSON | 1394 |
| Ulteriori informazioni | 1394 |
| AWSArtifactAccountSync | 1394 |
| Utilizzo di questa politica | 1394 |
| Dettagli della politica | 1394 |
| Versione della politica | 1395 |
| Documento di policy JSON | 1395 |
| Ulteriori informazioni | 1395 |
| AWSArtifactReportsReadOnlyAccess | 1395 |
| Utilizzo di questa politica | 1396 |
| Dettagli della politica | 1396 |
| Versione della politica | 1396 |
| Documento di policy JSON | 1396 |
| Ulteriori informazioni | 1397 |
| AWSArtifactServiceRolePolicy | 1397 |
| Utilizzo di questa politica | 1397 |
| Dettagli della politica | 1397 |
| Versione della politica | 1397 |
| Documento di policy JSON | 1398 |
| Ulteriori informazioni | 1398 |
| AWSAuditManagerAdministratorAccess | 1398 |
| Utilizzo di questa politica | 1398 |
| Dettagli della politica | 1398 |
| Versione della politica | 1399 |
| Documento di policy JSON | 1399 |
| Ulteriori informazioni | 1403 |

| | |
|--|------|
| AWSAuditManagerServiceRolePolicy | 1403 |
| Utilizzo di questa politica | 1403 |
| Dettagli della politica | 1403 |
| Versione della politica | 1403 |
| Documento di policy JSON | 1404 |
| Ulteriori informazioni | 1410 |
| AWSAutoScalingPlansEC2AutoScalingPolicy | 1411 |
| Utilizzo di questa politica | 1411 |
| Dettagli della politica | 1411 |
| Versione della politica | 1411 |
| Documento di policy JSON | 1411 |
| Ulteriori informazioni | 1412 |
| AWSBackupAuditAccess | 1412 |
| Utilizzo di questa politica | 1412 |
| Dettagli della politica | 1412 |
| Versione della politica | 1413 |
| Documento di policy JSON | 1413 |
| Ulteriori informazioni | 1414 |
| AWSBackupDataTransferAccess | 1414 |
| Utilizzo di questa politica | 1414 |
| Dettagli della politica | 1414 |
| Versione della politica | 1415 |
| Documento di policy JSON | 1415 |
| Ulteriori informazioni | 1415 |
| AWSBackupFullAccess | 1416 |
| Utilizzo di questa politica | 1416 |
| Dettagli della politica | 1416 |
| Versione della politica | 1416 |
| Documento di policy JSON | 1416 |
| Ulteriori informazioni | 1426 |
| AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync | 1426 |
| Utilizzo di questa politica | 1426 |
| Dettagli della politica | 1426 |
| Versione della politica | 1427 |
| Documento di policy JSON | 1427 |
| Ulteriori informazioni | 1428 |

| | |
|---|------|
| AWSBackupOperatorAccess | 1428 |
| Utilizzo di questa politica | 1428 |
| Dettagli della politica | 1428 |
| Versione della politica | 1428 |
| Documento di policy JSON | 1428 |
| Ulteriori informazioni | 1435 |
| AWSBackupOrganizationAdminAccess | 1435 |
| Utilizzo di questa politica | 1436 |
| Dettagli della politica | 1436 |
| Versione della politica | 1436 |
| Documento di policy JSON | 1436 |
| Ulteriori informazioni | 1438 |
| AWSBackupRestoreAccessForSAPHANA | 1438 |
| Utilizzo di questa politica | 1438 |
| Dettagli della politica | 1438 |
| Versione della politica | 1439 |
| Documento di policy JSON | 1439 |
| Ulteriori informazioni | 1440 |
| AWSBackupServiceLinkedRolePolicyForBackup | 1440 |
| Utilizzo di questa politica | 1440 |
| Dettagli della politica | 1440 |
| Versione della politica | 1440 |
| Documento di policy JSON | 1441 |
| Ulteriori informazioni | 1449 |
| AWSBackupServiceLinkedRolePolicyForBackupTest | 1449 |
| Utilizzo di questa politica | 1449 |
| Dettagli della politica | 1449 |
| Versione della politica | 1449 |
| Documento di policy JSON | 1449 |
| Ulteriori informazioni | 1450 |
| AWSBackupServiceRolePolicyForBackup | 1450 |
| Utilizzo di questa politica | 1450 |
| Dettagli della politica | 1451 |
| Versione della politica | 1451 |
| Documento di policy JSON | 1451 |
| Ulteriori informazioni | 1462 |

| | |
|--|------|
| AWSBackupServiceRolePolicyForRestores | 1462 |
| Utilizzo di questa politica | 1462 |
| Dettagli della politica | 1462 |
| Versione della politica | 1463 |
| Documento di policy JSON | 1463 |
| Ulteriori informazioni | 1473 |
| AWSBackupServiceRolePolicyForS3Backup | 1473 |
| Utilizzo di questa politica | 1473 |
| Dettagli della politica | 1473 |
| Versione della politica | 1473 |
| Documento di policy JSON | 1474 |
| Ulteriori informazioni | 1476 |
| AWSBackupServiceRolePolicyForS3Restore | 1476 |
| Utilizzo di questa politica | 1476 |
| Dettagli della politica | 1476 |
| Versione della politica | 1477 |
| Documento di policy JSON | 1477 |
| Ulteriori informazioni | 1478 |
| AWSBatchFullAccess | 1478 |
| Utilizzo di questa politica | 1478 |
| Dettagli della politica | 1479 |
| Versione della politica | 1479 |
| Documento di policy JSON | 1479 |
| Ulteriori informazioni | 1480 |
| AWSBatchServiceEventTargetRole | 1481 |
| Utilizzo di questa politica | 1481 |
| Dettagli della politica | 1481 |
| Versione della politica | 1481 |
| Documento di policy JSON | 1481 |
| Ulteriori informazioni | 1482 |
| AWSBatchServiceRole | 1482 |
| Utilizzo di questa politica | 1482 |
| Dettagli della politica | 1482 |
| Versione della politica | 1482 |
| Documento di policy JSON | 1482 |
| Ulteriori informazioni | 1486 |

| | |
|--|------|
| AWSBCMDDataExportsServiceRolePolicy | 1486 |
| Utilizzo di questa politica | 1486 |
| Dettagli della politica | 1486 |
| Versione della politica | 1486 |
| Documento di policy JSON | 1487 |
| Ulteriori informazioni | 1487 |
| AWSBillingConductorFullAccess | 1487 |
| Utilizzo di questa politica | 1487 |
| Dettagli della politica | 1487 |
| Versione della politica | 1488 |
| Documento di policy JSON | 1488 |
| Ulteriori informazioni | 1488 |
| AWSBillingConductorReadOnlyAccess | 1488 |
| Utilizzo di questa politica | 1489 |
| Dettagli della politica | 1489 |
| Versione della politica | 1489 |
| Documento di policy JSON | 1489 |
| Ulteriori informazioni | 1490 |
| AWSBillingReadOnlyAccess | 1490 |
| Utilizzo di questa politica | 1490 |
| Dettagli della politica | 1490 |
| Versione della politica | 1490 |
| Documento di policy JSON | 1490 |
| Ulteriori informazioni | 1492 |
| AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM | 1492 |
| Utilizzo di questa politica | 1492 |
| Dettagli della politica | 1492 |
| Versione della politica | 1493 |
| Documento di policy JSON | 1493 |
| Ulteriori informazioni | 1494 |
| AWSBudgetsActionsWithAWSResourceControlAccess | 1494 |
| Utilizzo di questa politica | 1494 |
| Dettagli della politica | 1494 |
| Versione della politica | 1495 |
| Documento di policy JSON | 1495 |
| Ulteriori informazioni | 1496 |

| | |
|---|------|
| AWSBudgetsReadOnlyAccess | 1496 |
| Utilizzo di questa politica | 1496 |
| Dettagli della politica | 1496 |
| Versione della politica | 1497 |
| Documento di policy JSON | 1497 |
| Ulteriori informazioni | 1497 |
| AWSBugBustFullAccess | 1497 |
| Utilizzo di questa politica | 1498 |
| Dettagli della politica | 1498 |
| Versione della politica | 1498 |
| Documento di policy JSON | 1498 |
| Ulteriori informazioni | 1499 |
| AWSBugBustPlayerAccess | 1499 |
| Utilizzo di questa politica | 1500 |
| Dettagli della politica | 1500 |
| Versione della politica | 1500 |
| Documento di policy JSON | 1500 |
| Ulteriori informazioni | 1501 |
| AWSBugBustServiceRolePolicy | 1501 |
| Utilizzo di questa politica | 1501 |
| Dettagli della politica | 1502 |
| Versione della politica | 1502 |
| Documento di policy JSON | 1502 |
| Ulteriori informazioni | 1502 |
| AWSCertificateManagerFullAccess | 1503 |
| Utilizzo di questa politica | 1503 |
| Dettagli della politica | 1503 |
| Versione della politica | 1503 |
| Documento di policy JSON | 1503 |
| Ulteriori informazioni | 1504 |
| AWSCertificateManagerPrivateCAAuditor | 1504 |
| Utilizzo di questa politica | 1505 |
| Dettagli della politica | 1505 |
| Versione della politica | 1505 |
| Documento di policy JSON | 1505 |
| Ulteriori informazioni | 1506 |

| | |
|--|------|
| AWSCertificateManagerPrivateCAFullAccess | 1506 |
| Utilizzo di questa politica | 1506 |
| Dettagli della politica | 1506 |
| Versione della politica | 1506 |
| Documento di policy JSON | 1507 |
| Ulteriori informazioni | 1507 |
| AWSCertificateManagerPrivateCAPrivilegedUser | 1507 |
| Utilizzo di questa politica | 1507 |
| Dettagli della politica | 1508 |
| Versione della politica | 1508 |
| Documento di policy JSON | 1508 |
| Ulteriori informazioni | 1509 |
| AWSCertificateManagerPrivateCAReadOnly | 1509 |
| Utilizzo di questa politica | 1510 |
| Dettagli della politica | 1510 |
| Versione della politica | 1510 |
| Documento di policy JSON | 1510 |
| Ulteriori informazioni | 1511 |
| AWSCertificateManagerPrivateCAUser | 1511 |
| Utilizzo di questa politica | 1511 |
| Dettagli della politica | 1511 |
| Versione della politica | 1511 |
| Documento di policy JSON | 1511 |
| Ulteriori informazioni | 1513 |
| AWSCertificateManagerReadOnly | 1513 |
| Utilizzo di questa politica | 1513 |
| Dettagli della politica | 1513 |
| Versione della politica | 1513 |
| Documento di policy JSON | 1514 |
| Ulteriori informazioni | 1514 |
| AWSChatbotServiceLinkedRolePolicy | 1514 |
| Utilizzo di questa politica | 1514 |
| Dettagli della politica | 1514 |
| Versione della politica | 1515 |
| Documento di policy JSON | 1515 |
| Ulteriori informazioni | 1516 |

| | |
|---|------|
| AWSCleanRoomsFullAccess | 1516 |
| Utilizzo di questa politica | 1516 |
| Dettagli della politica | 1516 |
| Versione della politica | 1516 |
| Documento di policy JSON | 1516 |
| Ulteriori informazioni | 1521 |
| AWSCleanRoomsFullAccessNoQuerying | 1521 |
| Utilizzo di questa politica | 1521 |
| Dettagli della politica | 1521 |
| Versione della politica | 1521 |
| Documento di policy JSON | 1522 |
| Ulteriori informazioni | 1526 |
| AWSCleanRoomsMLFullAccess | 1527 |
| Utilizzo di questa politica | 1527 |
| Dettagli della politica | 1527 |
| Versione della politica | 1527 |
| Documento di policy JSON | 1527 |
| Ulteriori informazioni | 1531 |
| AWSCleanRoomsMLReadOnlyAccess | 1531 |
| Utilizzo di questa politica | 1531 |
| Dettagli della politica | 1531 |
| Versione della politica | 1531 |
| Documento di policy JSON | 1532 |
| Ulteriori informazioni | 1533 |
| AWSCleanRoomsReadOnlyAccess | 1533 |
| Utilizzo di questa politica | 1533 |
| Dettagli della politica | 1533 |
| Versione della politica | 1533 |
| Documento di policy JSON | 1533 |
| Ulteriori informazioni | 1535 |
| AWSCloud9Administrator | 1535 |
| Utilizzo di questa politica | 1535 |
| Dettagli della politica | 1535 |
| Versione della politica | 1535 |
| Documento di policy JSON | 1535 |
| Ulteriori informazioni | 1537 |

| | |
|---------------------------------------|------|
| AWSCloud9EnvironmentMember | 1537 |
| Utilizzo di questa politica | 1537 |
| Dettagli della politica | 1537 |
| Versione della politica | 1537 |
| Documento di policy JSON | 1538 |
| Ulteriori informazioni | 1539 |
| AWSCloud9ServiceRolePolicy | 1539 |
| Utilizzo di questa politica | 1539 |
| Dettagli della politica | 1539 |
| Versione della politica | 1540 |
| Documento di policy JSON | 1540 |
| Ulteriori informazioni | 1542 |
| AWSCloud9SSMInstanceProfile | 1542 |
| Utilizzo di questa politica | 1543 |
| Dettagli della politica | 1543 |
| Versione della politica | 1543 |
| Documento di policy JSON | 1543 |
| Ulteriori informazioni | 1544 |
| AWSCloud9User | 1544 |
| Utilizzo di questa politica | 1544 |
| Dettagli della politica | 1544 |
| Versione della politica | 1544 |
| Documento di policy JSON | 1544 |
| Ulteriori informazioni | 1547 |
| AWSCloudFormationFullAccess | 1547 |
| Utilizzo di questa politica | 1547 |
| Dettagli della politica | 1547 |
| Versione della politica | 1547 |
| Documento di policy JSON | 1548 |
| Ulteriori informazioni | 1548 |
| AWSCloudFormationReadOnlyAccess | 1548 |
| Utilizzo di questa politica | 1548 |
| Dettagli della politica | 1548 |
| Versione della politica | 1549 |
| Documento di policy JSON | 1549 |
| Ulteriori informazioni | 1549 |

| | |
|---|------|
| AWSCloudFrontLogger | 1549 |
| Utilizzo di questa politica | 1550 |
| Dettagli della politica | 1550 |
| Versione della politica | 1550 |
| Documento di policy JSON | 1550 |
| Ulteriori informazioni | 1551 |
| AWSCloudHSMFullAccess | 1551 |
| Utilizzo di questa politica | 1551 |
| Dettagli della politica | 1551 |
| Versione della politica | 1551 |
| Documento di policy JSON | 1551 |
| Ulteriori informazioni | 1552 |
| AWSCloudHSMReadOnlyAccess | 1552 |
| Utilizzo di questa politica | 1552 |
| Dettagli della politica | 1552 |
| Versione della politica | 1552 |
| Documento di policy JSON | 1553 |
| Ulteriori informazioni | 1553 |
| AWSCloudHSMRole | 1553 |
| Utilizzo di questa politica | 1553 |
| Dettagli della politica | 1553 |
| Versione della politica | 1554 |
| Documento di policy JSON | 1554 |
| Ulteriori informazioni | 1554 |
| AWSCloudMapDiscoverInstanceAccess | 1555 |
| Utilizzo di questa politica | 1555 |
| Dettagli della politica | 1555 |
| Versione della politica | 1555 |
| Documento di policy JSON | 1555 |
| Ulteriori informazioni | 1556 |
| AWSCloudMapFullAccess | 1556 |
| Utilizzo di questa politica | 1556 |
| Dettagli della politica | 1556 |
| Versione della politica | 1556 |
| Documento di policy JSON | 1557 |
| Ulteriori informazioni | 1557 |

| | |
|---|------|
| AWSCloudMapReadOnlyAccess | 1557 |
| Utilizzo di questa politica | 1558 |
| Dettagli della politica | 1558 |
| Versione della politica | 1558 |
| Documento di policy JSON | 1558 |
| Ulteriori informazioni | 1559 |
| AWSCloudMapRegisterInstanceAccess | 1559 |
| Utilizzo di questa politica | 1559 |
| Dettagli della politica | 1559 |
| Versione della politica | 1559 |
| Documento di policy JSON | 1559 |
| Ulteriori informazioni | 1560 |
| AWSCloudShellFullAccess | 1560 |
| Utilizzo di questa politica | 1560 |
| Dettagli della politica | 1561 |
| Versione della politica | 1561 |
| Documento di policy JSON | 1561 |
| Ulteriori informazioni | 1561 |
| AWSCloudTrail_FullAccess | 1562 |
| Utilizzo di questa politica | 1562 |
| Dettagli della politica | 1562 |
| Versione della politica | 1562 |
| Documento di policy JSON | 1562 |
| Ulteriori informazioni | 1565 |
| AWSCloudTrail_ReadOnlyAccess | 1565 |
| Utilizzo di questa politica | 1565 |
| Dettagli della politica | 1565 |
| Versione della politica | 1565 |
| Documento di policy JSON | 1566 |
| Ulteriori informazioni | 1566 |
| AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy | 1566 |
| Utilizzo di questa politica | 1566 |
| Dettagli della politica | 1567 |
| Versione della politica | 1567 |
| Documento di policy JSON | 1567 |
| Ulteriori informazioni | 1567 |

| | |
|-------------------------------------|------|
| AWSCodeArtifactAdminAccess | 1567 |
| Utilizzo di questa politica | 1568 |
| Dettagli della politica | 1568 |
| Versione della politica | 1568 |
| Documento di policy JSON | 1568 |
| Ulteriori informazioni | 1569 |
| AWSCodeArtifactReadOnlyAccess | 1569 |
| Utilizzo di questa politica | 1569 |
| Dettagli della politica | 1569 |
| Versione della politica | 1569 |
| Documento di policy JSON | 1570 |
| Ulteriori informazioni | 1570 |
| AWSCodeBuildAdminAccess | 1571 |
| Utilizzo di questa politica | 1571 |
| Dettagli della politica | 1571 |
| Versione della politica | 1571 |
| Documento di policy JSON | 1571 |
| Ulteriori informazioni | 1575 |
| AWSCodeBuildDeveloperAccess | 1575 |
| Utilizzo di questa politica | 1575 |
| Dettagli della politica | 1575 |
| Versione della politica | 1575 |
| Documento di policy JSON | 1575 |
| Ulteriori informazioni | 1578 |
| AWSCodeBuildReadOnlyAccess | 1578 |
| Utilizzo di questa politica | 1578 |
| Dettagli della politica | 1579 |
| Versione della politica | 1579 |
| Documento di policy JSON | 1579 |
| Ulteriori informazioni | 1580 |
| AWSCodeCommitFullAccess | 1581 |
| Utilizzo di questa politica | 1581 |
| Dettagli della politica | 1581 |
| Versione della politica | 1581 |
| Documento di policy JSON | 1581 |
| Ulteriori informazioni | 1586 |

| | |
|-----------------------------------|------|
| AWSCodeCommitPowerUser | 1586 |
| Utilizzo di questa politica | 1586 |
| Dettagli della politica | 1586 |
| Versione della politica | 1587 |
| Documento di policy JSON | 1587 |
| Ulteriori informazioni | 1591 |
| AWSCodeCommitReadOnly | 1592 |
| Utilizzo di questa politica | 1592 |
| Dettagli della politica | 1592 |
| Versione della politica | 1592 |
| Documento di policy JSON | 1592 |
| Ulteriori informazioni | 1595 |
| AWSCodeDeployDeployerAccess | 1595 |
| Utilizzo di questa politica | 1595 |
| Dettagli della politica | 1595 |
| Versione della politica | 1596 |
| Documento di policy JSON | 1596 |
| Ulteriori informazioni | 1597 |
| AWSCodeDeployFullAccess | 1597 |
| Utilizzo di questa politica | 1598 |
| Dettagli della politica | 1598 |
| Versione della politica | 1598 |
| Documento di policy JSON | 1598 |
| Ulteriori informazioni | 1600 |
| AWSCodeDeployReadOnlyAccess | 1600 |
| Utilizzo di questa politica | 1600 |
| Dettagli della politica | 1600 |
| Versione della politica | 1600 |
| Documento di policy JSON | 1600 |
| Ulteriori informazioni | 1601 |
| AWSCodeDeployRole | 1602 |
| Utilizzo di questa politica | 1602 |
| Dettagli della politica | 1602 |
| Versione della politica | 1602 |
| Documento di policy JSON | 1602 |
| Ulteriori informazioni | 1604 |

| | |
|--|------|
| AWSCodeDeployRoleForCloudFormation | 1604 |
| Utilizzo di questa politica | 1604 |
| Dettagli della politica | 1604 |
| Versione della politica | 1604 |
| Documento di policy JSON | 1604 |
| Ulteriori informazioni | 1605 |
| AWSCodeDeployRoleForECS | 1605 |
| Utilizzo di questa politica | 1605 |
| Dettagli della politica | 1605 |
| Versione della politica | 1606 |
| Documento di policy JSON | 1606 |
| Ulteriori informazioni | 1607 |
| AWSCodeDeployRoleForECSLimited | 1607 |
| Utilizzo di questa politica | 1607 |
| Dettagli della politica | 1607 |
| Versione della politica | 1607 |
| Documento di policy JSON | 1608 |
| Ulteriori informazioni | 1609 |
| AWSCodeDeployRoleForLambda | 1610 |
| Utilizzo di questa politica | 1610 |
| Dettagli della politica | 1610 |
| Versione della politica | 1610 |
| Documento di policy JSON | 1610 |
| Ulteriori informazioni | 1611 |
| AWSCodeDeployRoleForLambdaLimited | 1612 |
| Utilizzo di questa politica | 1612 |
| Dettagli della politica | 1612 |
| Versione della politica | 1612 |
| Documento di policy JSON | 1612 |
| Ulteriori informazioni | 1613 |
| AWSCodePipeline_FullAccess | 1614 |
| Utilizzo di questa politica | 1614 |
| Dettagli della politica | 1614 |
| Versione della politica | 1614 |
| Documento di policy JSON | 1614 |
| Ulteriori informazioni | 1618 |

| | |
|---|------|
| AWSCodePipeline_ReadOnlyAccess | 1618 |
| Utilizzo di questa politica | 1618 |
| Dettagli della politica | 1618 |
| Versione della politica | 1619 |
| Documento di policy JSON | 1619 |
| Ulteriori informazioni | 1620 |
| AWSCodePipelineApproverAccess | 1620 |
| Utilizzo di questa politica | 1620 |
| Dettagli della politica | 1620 |
| Versione della politica | 1621 |
| Documento di policy JSON | 1621 |
| Ulteriori informazioni | 1621 |
| AWSCodePipelineCustomActionAccess | 1621 |
| Utilizzo di questa politica | 1622 |
| Dettagli della politica | 1622 |
| Versione della politica | 1622 |
| Documento di policy JSON | 1622 |
| Ulteriori informazioni | 1623 |
| AWSCodeStarFullAccess | 1623 |
| Utilizzo di questa politica | 1623 |
| Dettagli della politica | 1623 |
| Versione della politica | 1623 |
| Documento di policy JSON | 1623 |
| Ulteriori informazioni | 1624 |
| AWSCodeStarNotificationsServiceRolePolicy | 1624 |
| Utilizzo di questa politica | 1625 |
| Dettagli della politica | 1625 |
| Versione della politica | 1625 |
| Documento di policy JSON | 1625 |
| Ulteriori informazioni | 1626 |
| AWSCodeStarServiceRole | 1626 |
| Utilizzo di questa politica | 1627 |
| Dettagli della politica | 1627 |
| Versione della politica | 1627 |
| Documento di policy JSON | 1627 |
| Ulteriori informazioni | 1632 |

| | |
|---|------|
| AWSCompromisedKeyQuarantine | 1632 |
| Utilizzo di questa politica | 1632 |
| Dettagli della politica | 1632 |
| Versione della politica | 1633 |
| Documento di policy JSON | 1633 |
| Ulteriori informazioni | 1634 |
| AWSCompromisedKeyQuarantineV2 | 1634 |
| Utilizzo di questa politica | 1634 |
| Dettagli della politica | 1634 |
| Versione della politica | 1635 |
| Documento di policy JSON | 1635 |
| Ulteriori informazioni | 1637 |
| AWSConfigMultiAccountSetupPolicy | 1637 |
| Utilizzo di questa politica | 1637 |
| Dettagli della politica | 1637 |
| Versione della politica | 1637 |
| Documento di policy JSON | 1638 |
| Ulteriori informazioni | 1639 |
| AWSConfigRemediationServiceRolePolicy | 1640 |
| Utilizzo di questa politica | 1640 |
| Dettagli della politica | 1640 |
| Versione della politica | 1640 |
| Documento di policy JSON | 1640 |
| Ulteriori informazioni | 1641 |
| AWSConfigRoleForOrganizations | 1641 |
| Utilizzo di questa politica | 1641 |
| Dettagli della politica | 1641 |
| Versione della politica | 1642 |
| Documento di policy JSON | 1642 |
| Ulteriori informazioni | 1642 |
| AWSConfigRulesExecutionRole | 1642 |
| Utilizzo di questa politica | 1643 |
| Dettagli della politica | 1643 |
| Versione della politica | 1643 |
| Documento di policy JSON | 1643 |
| Ulteriori informazioni | 1644 |

| | |
|---|------|
| AWSConfigServiceRolePolicy | 1644 |
| Utilizzo di questa politica | 1644 |
| Dettagli della politica | 1644 |
| Versione della politica | 1644 |
| Documento di policy JSON | 1645 |
| Ulteriori informazioni | 1676 |
| AWSConfigUserAccess | 1676 |
| Utilizzo di questa politica | 1676 |
| Dettagli della politica | 1677 |
| Versione della politica | 1677 |
| Documento di policy JSON | 1677 |
| Ulteriori informazioni | 1678 |
| AWSConnector | 1678 |
| Utilizzo di questa politica | 1678 |
| Dettagli della politica | 1678 |
| Versione della politica | 1678 |
| Documento di policy JSON | 1678 |
| Ulteriori informazioni | 1680 |
| AWSControlTowerAccountServiceRolePolicy | 1681 |
| Utilizzo di questa politica | 1681 |
| Dettagli della politica | 1681 |
| Versione della politica | 1681 |
| Documento di policy JSON | 1681 |
| Ulteriori informazioni | 1683 |
| AWSControlTowerServiceRolePolicy | 1683 |
| Utilizzo di questa politica | 1683 |
| Dettagli della politica | 1683 |
| Versione della politica | 1684 |
| Documento di policy JSON | 1684 |
| Ulteriori informazioni | 1688 |
| AWSCostAndUsageReportAutomationPolicy | 1688 |
| Utilizzo di questa politica | 1689 |
| Dettagli della politica | 1689 |
| Versione della politica | 1689 |
| Documento di policy JSON | 1689 |
| Ulteriori informazioni | 1690 |

| | |
|--|------|
| AWSDataExchangeFullAccess | 1690 |
| Utilizzo di questa politica | 1690 |
| Dettagli della politica | 1691 |
| Versione della politica | 1691 |
| Documento di policy JSON | 1691 |
| Ulteriori informazioni | 1694 |
| AWSDataExchangeProviderFullAccess | 1695 |
| Utilizzo di questa politica | 1695 |
| Dettagli della politica | 1695 |
| Versione della politica | 1695 |
| Documento di policy JSON | 1695 |
| Ulteriori informazioni | 1699 |
| AWSDataExchangeReadOnly | 1699 |
| Utilizzo di questa politica | 1699 |
| Dettagli della politica | 1699 |
| Versione della politica | 1700 |
| Documento di policy JSON | 1700 |
| Ulteriori informazioni | 1701 |
| AWSDataExchangeSubscriberFullAccess | 1701 |
| Utilizzo di questa politica | 1701 |
| Dettagli della politica | 1701 |
| Versione della politica | 1701 |
| Documento di policy JSON | 1701 |
| Ulteriori informazioni | 1704 |
| AWSDataLifecycleManagerServiceRole | 1704 |
| Utilizzo di questa politica | 1704 |
| Dettagli della politica | 1704 |
| Versione della politica | 1704 |
| Documento di policy JSON | 1705 |
| Ulteriori informazioni | 1706 |
| AWSDataLifecycleManagerServiceRoleForAMIManagement | 1706 |
| Utilizzo di questa politica | 1706 |
| Dettagli della politica | 1706 |
| Versione della politica | 1706 |
| Documento di policy JSON | 1707 |
| Ulteriori informazioni | 1708 |

| | |
|---|------|
| AWSDatalifecycleManagerSSMFullAccess | 1708 |
| Utilizzo di questa politica | 1708 |
| Dettagli della politica | 1708 |
| Versione della politica | 1709 |
| Documento di policy JSON | 1709 |
| Ulteriori informazioni | 1710 |
| AWSDatapipeline_FullAccess | 1710 |
| Utilizzo di questa politica | 1710 |
| Dettagli della politica | 1711 |
| Versione della politica | 1711 |
| Documento di policy JSON | 1711 |
| Ulteriori informazioni | 1712 |
| AWSDatapipeline_PowerUser | 1712 |
| Utilizzo di questa politica | 1712 |
| Dettagli della politica | 1712 |
| Versione della politica | 1713 |
| Documento di policy JSON | 1713 |
| Ulteriori informazioni | 1714 |
| AWSDatasyncDiscoveryServiceRolePolicy | 1714 |
| Utilizzo di questa politica | 1714 |
| Dettagli della politica | 1714 |
| Versione della politica | 1714 |
| Documento di policy JSON | 1715 |
| Ulteriori informazioni | 1716 |
| AWSDatasyncFullAccess | 1716 |
| Utilizzo di questa politica | 1716 |
| Dettagli della politica | 1716 |
| Versione della politica | 1716 |
| Documento di policy JSON | 1716 |
| Ulteriori informazioni | 1718 |
| AWSDatasyncReadOnlyAccess | 1718 |
| Utilizzo di questa politica | 1718 |
| Dettagli della politica | 1718 |
| Versione della politica | 1718 |
| Documento di policy JSON | 1719 |
| Ulteriori informazioni | 1719 |

| | |
|---|------|
| AWSDeadlineCloud-FleetWorker | 1719 |
| Utilizzo di questa politica | 1720 |
| Dettagli della politica | 1720 |
| Versione della politica | 1720 |
| Documento di policy JSON | 1720 |
| Ulteriori informazioni | 1721 |
| AWSDeadlineCloud-UserAccessFarms | 1721 |
| Utilizzo di questa politica | 1721 |
| Dettagli della politica | 1721 |
| Versione della politica | 1721 |
| Documento di policy JSON | 1722 |
| Ulteriori informazioni | 1727 |
| AWSDeadlineCloud-UserAccessFleets | 1727 |
| Utilizzo di questa politica | 1727 |
| Dettagli della politica | 1727 |
| Versione della politica | 1727 |
| Documento di policy JSON | 1728 |
| Ulteriori informazioni | 1731 |
| AWSDeadlineCloud-UserAccessJobs | 1732 |
| Utilizzo di questa politica | 1732 |
| Dettagli della politica | 1732 |
| Versione della politica | 1732 |
| Documento di policy JSON | 1732 |
| Ulteriori informazioni | 1736 |
| AWSDeadlineCloud-UserAccessQueues | 1736 |
| Utilizzo di questa politica | 1736 |
| Dettagli della politica | 1737 |
| Versione della politica | 1737 |
| Documento di policy JSON | 1737 |
| Ulteriori informazioni | 1742 |
| AWSDeadlineCloud-WorkerHost | 1742 |
| Utilizzo di questa politica | 1742 |
| Dettagli della politica | 1742 |
| Versione della politica | 1742 |
| Documento di policy JSON | 1742 |
| Ulteriori informazioni | 1743 |

| | |
|--|------|
| AWSDeepLensLambdaFunctionAccessPolicy | 1743 |
| Utilizzo di questa politica | 1743 |
| Dettagli della politica | 1743 |
| Versione della politica | 1744 |
| Documento di policy JSON | 1744 |
| Ulteriori informazioni | 1745 |
| AWSDeepLensServiceRolePolicy | 1745 |
| Utilizzo di questa politica | 1745 |
| Dettagli della politica | 1746 |
| Versione della politica | 1746 |
| Documento di policy JSON | 1746 |
| Ulteriori informazioni | 1753 |
| AWSDeepRacerAccountAdminAccess | 1753 |
| Utilizzo di questa politica | 1753 |
| Dettagli della politica | 1753 |
| Versione della politica | 1754 |
| Documento di policy JSON | 1754 |
| Ulteriori informazioni | 1754 |
| AWSDeepRacerCloudFormationAccessPolicy | 1755 |
| Utilizzo di questa politica | 1755 |
| Dettagli della politica | 1755 |
| Versione della politica | 1755 |
| Documento di policy JSON | 1755 |
| Ulteriori informazioni | 1758 |
| AWSDeepRacerDefaultMultiUserAccess | 1758 |
| Utilizzo di questa politica | 1759 |
| Dettagli della politica | 1759 |
| Versione della politica | 1759 |
| Documento di policy JSON | 1759 |
| Ulteriori informazioni | 1760 |
| AWSDeepRacerFullAccess | 1761 |
| Utilizzo di questa politica | 1761 |
| Dettagli della politica | 1761 |
| Versione della politica | 1761 |
| Documento di policy JSON | 1761 |
| Ulteriori informazioni | 1762 |

| | |
|--|------|
| AWSDeepRacerRoboMakerAccessPolicy | 1763 |
| Utilizzo di questa politica | 1763 |
| Dettagli della politica | 1763 |
| Versione della politica | 1763 |
| Documento di policy JSON | 1763 |
| Ulteriori informazioni | 1765 |
| AWSDeepRacerServiceRolePolicy | 1765 |
| Utilizzo di questa politica | 1766 |
| Dettagli della politica | 1766 |
| Versione della politica | 1766 |
| Documento di policy JSON | 1766 |
| Ulteriori informazioni | 1769 |
| AWSDenyAll | 1769 |
| Utilizzo di questa politica | 1769 |
| Dettagli della politica | 1770 |
| Versione della politica | 1770 |
| Documento di policy JSON | 1770 |
| Ulteriori informazioni | 1770 |
| AWSDeviceFarmFullAccess | 1771 |
| Utilizzo di questa politica | 1771 |
| Dettagli della politica | 1771 |
| Versione della politica | 1771 |
| Documento di policy JSON | 1771 |
| Ulteriori informazioni | 1772 |
| AWSDeviceFarmServiceRolePolicy | 1772 |
| Utilizzo di questa politica | 1772 |
| Dettagli della politica | 1772 |
| Versione della politica | 1772 |
| Documento di policy JSON | 1773 |
| Ulteriori informazioni | 1775 |
| AWSDeviceFarmTestGridServiceRolePolicy | 1775 |
| Utilizzo di questa politica | 1775 |
| Dettagli della politica | 1775 |
| Versione della politica | 1775 |
| Documento di policy JSON | 1775 |
| Ulteriori informazioni | 1778 |

| | |
|--|------|
| AWSDirectConnectFullAccess | 1778 |
| Utilizzo di questa politica | 1778 |
| Dettagli della politica | 1778 |
| Versione della politica | 1778 |
| Documento di policy JSON | 1778 |
| Ulteriori informazioni | 1779 |
| AWSDirectConnectReadOnlyAccess | 1779 |
| Utilizzo di questa politica | 1779 |
| Dettagli della politica | 1779 |
| Versione della politica | 1779 |
| Documento di policy JSON | 1780 |
| Ulteriori informazioni | 1780 |
| AWSDirectConnectServiceRolePolicy | 1780 |
| Utilizzo di questa politica | 1781 |
| Dettagli della politica | 1781 |
| Versione della politica | 1781 |
| Documento di policy JSON | 1781 |
| Ulteriori informazioni | 1782 |
| AWSDirectoryServiceFullAccess | 1782 |
| Utilizzo di questa politica | 1782 |
| Dettagli della politica | 1782 |
| Versione della politica | 1782 |
| Documento di policy JSON | 1782 |
| Ulteriori informazioni | 1784 |
| AWSDirectoryServiceReadOnlyAccess | 1784 |
| Utilizzo di questa politica | 1785 |
| Dettagli della politica | 1785 |
| Versione della politica | 1785 |
| Documento di policy JSON | 1785 |
| Ulteriori informazioni | 1786 |
| AWSDiscoveryContinuousExportFirehosePolicy | 1786 |
| Utilizzo di questa politica | 1786 |
| Dettagli della politica | 1786 |
| Versione della politica | 1786 |
| Documento di policy JSON | 1787 |
| Ulteriori informazioni | 1788 |

| | |
|--|------|
| AWSDMSFleetAdvisorServiceRolePolicy | 1788 |
| Utilizzo di questa politica | 1788 |
| Dettagli della politica | 1788 |
| Versione della politica | 1788 |
| Documento di policy JSON | 1788 |
| Ulteriori informazioni | 1789 |
| AWSDMSServerlessServiceRolePolicy | 1789 |
| Utilizzo di questa politica | 1789 |
| Dettagli della politica | 1789 |
| Versione della politica | 1790 |
| Documento di policy JSON | 1790 |
| Ulteriori informazioni | 1791 |
| AWSEC2CapacityReservationFleetRolePolicy | 1791 |
| Utilizzo di questa politica | 1792 |
| Dettagli della politica | 1792 |
| Versione della politica | 1792 |
| Documento di policy JSON | 1792 |
| Ulteriori informazioni | 1793 |
| AWSEC2FleetServiceRolePolicy | 1793 |
| Utilizzo di questa politica | 1794 |
| Dettagli della politica | 1794 |
| Versione della politica | 1794 |
| Documento di policy JSON | 1794 |
| Ulteriori informazioni | 1796 |
| AWSEC2SpotFleetServiceRolePolicy | 1796 |
| Utilizzo di questa politica | 1796 |
| Dettagli della politica | 1797 |
| Versione della politica | 1797 |
| Documento di policy JSON | 1797 |
| Ulteriori informazioni | 1799 |
| AWSEC2SpotServiceRolePolicy | 1799 |
| Utilizzo di questa politica | 1799 |
| Dettagli della politica | 1799 |
| Versione della politica | 1799 |
| Documento di policy JSON | 1800 |
| Ulteriori informazioni | 1801 |

| | |
|---|------|
| AWSEC2VssSnapshotPolicy | 1801 |
| Utilizzo di questa politica | 1801 |
| Dettagli della politica | 1802 |
| Versione della politica | 1802 |
| Documento di policy JSON | 1802 |
| Ulteriori informazioni | 1805 |
| AWSECRPullThroughCache_ServiceRolePolicy | 1805 |
| Utilizzo di questa politica | 1806 |
| Dettagli della politica | 1806 |
| Versione della politica | 1806 |
| Documento di policy JSON | 1806 |
| Ulteriori informazioni | 1807 |
| AWSElasticBeanstalkCustomPlatformforEC2Role | 1807 |
| Utilizzo di questa politica | 1807 |
| Dettagli della politica | 1807 |
| Versione della politica | 1808 |
| Documento di policy JSON | 1808 |
| Ulteriori informazioni | 1809 |
| AWSElasticBeanstalkEnhancedHealth | 1810 |
| Utilizzo di questa politica | 1810 |
| Dettagli della politica | 1810 |
| Versione della politica | 1810 |
| Documento di policy JSON | 1810 |
| Ulteriori informazioni | 1811 |
| AWSElasticBeanstalkMaintenance | 1811 |
| Utilizzo di questa politica | 1812 |
| Dettagli della politica | 1812 |
| Versione della politica | 1812 |
| Documento di policy JSON | 1812 |
| Ulteriori informazioni | 1813 |
| AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy | 1813 |
| Utilizzo di questa politica | 1813 |
| Dettagli della politica | 1813 |
| Versione della politica | 1814 |
| Documento di policy JSON | 1814 |
| Ulteriori informazioni | 1820 |

| | |
|--|------|
| AWSElasticBeanstalkManagedUpdatesServiceRolePolicy | 1821 |
| Utilizzo di questa politica | 1821 |
| Dettagli della politica | 1821 |
| Versione della politica | 1821 |
| Documento di policy JSON | 1821 |
| Ulteriori informazioni | 1827 |
| AWSElasticBeanstalkMulticontainerDocker | 1827 |
| Utilizzo di questa politica | 1827 |
| Dettagli della politica | 1827 |
| Versione della politica | 1827 |
| Documento di policy JSON | 1827 |
| Ulteriori informazioni | 1828 |
| AWSElasticBeanstalkReadOnly | 1829 |
| Utilizzo di questa politica | 1829 |
| Dettagli della politica | 1829 |
| Versione della politica | 1829 |
| Documento di policy JSON | 1829 |
| Ulteriori informazioni | 1831 |
| AWSElasticBeanstalkRoleCore | 1832 |
| Utilizzo di questa politica | 1832 |
| Dettagli della politica | 1832 |
| Versione della politica | 1832 |
| Documento di policy JSON | 1832 |
| Ulteriori informazioni | 1837 |
| AWSElasticBeanstalkRoleCWL | 1837 |
| Utilizzo di questa politica | 1838 |
| Dettagli della politica | 1838 |
| Versione della politica | 1838 |
| Documento di policy JSON | 1838 |
| Ulteriori informazioni | 1839 |
| AWSElasticBeanstalkRoleECS | 1839 |
| Utilizzo di questa politica | 1839 |
| Dettagli della politica | 1839 |
| Versione della politica | 1839 |
| Documento di policy JSON | 1839 |
| Ulteriori informazioni | 1840 |

| | |
|--|------|
| AWSElasticBeanstalkRoleRDS | 1841 |
| Utilizzo di questa politica | 1841 |
| Dettagli della politica | 1841 |
| Versione della politica | 1841 |
| Documento di policy JSON | 1841 |
| Ulteriori informazioni | 1842 |
| AWSElasticBeanstalkRoleSNS | 1842 |
| Utilizzo di questa politica | 1842 |
| Dettagli della politica | 1842 |
| Versione della politica | 1842 |
| Documento di policy JSON | 1843 |
| Ulteriori informazioni | 1843 |
| AWSElasticBeanstalkRoleWorkerTier | 1844 |
| Utilizzo di questa politica | 1844 |
| Dettagli della politica | 1844 |
| Versione della politica | 1844 |
| Documento di policy JSON | 1844 |
| Ulteriori informazioni | 1845 |
| AWSElasticBeanstalkService | 1845 |
| Utilizzo di questa politica | 1845 |
| Dettagli della politica | 1845 |
| Versione della politica | 1846 |
| Documento di policy JSON | 1846 |
| Ulteriori informazioni | 1850 |
| AWSElasticBeanstalkServiceRolePolicy | 1850 |
| Utilizzo di questa politica | 1851 |
| Dettagli della politica | 1851 |
| Versione della politica | 1851 |
| Documento di policy JSON | 1851 |
| Ulteriori informazioni | 1853 |
| AWSElasticBeanstalkWebTier | 1853 |
| Utilizzo di questa politica | 1853 |
| Dettagli della politica | 1853 |
| Versione della politica | 1853 |
| Documento di policy JSON | 1853 |
| Ulteriori informazioni | 1855 |

| | |
|---|------|
| AWSElasticBeanstalkWorkerTier | 1855 |
| Utilizzo di questa politica | 1855 |
| Dettagli della politica | 1855 |
| Versione della politica | 1855 |
| Documento di policy JSON | 1856 |
| Ulteriori informazioni | 1858 |
| AWSElasticDisasterRecoveryAgentInstallationPolicy | 1858 |
| Utilizzo di questa politica | 1858 |
| Dettagli della politica | 1858 |
| Versione della politica | 1859 |
| Documento di policy JSON | 1859 |
| Ulteriori informazioni | 1860 |
| AWSElasticDisasterRecoveryAgentPolicy | 1860 |
| Utilizzo di questa politica | 1861 |
| Dettagli della politica | 1861 |
| Versione della politica | 1861 |
| Documento di policy JSON | 1861 |
| Ulteriori informazioni | 1862 |
| AWSElasticDisasterRecoveryConsoleFullAccess | 1862 |
| Utilizzo di questa politica | 1862 |
| Dettagli della politica | 1862 |
| Versione della politica | 1863 |
| Documento di policy JSON | 1863 |
| Ulteriori informazioni | 1872 |
| AWSElasticDisasterRecoveryConsoleFullAccess_v2 | 1873 |
| Utilizzo di questa politica | 1873 |
| Dettagli della politica | 1873 |
| Versione della politica | 1873 |
| Documento di policy JSON | 1873 |
| Ulteriori informazioni | 1886 |
| AWSElasticDisasterRecoveryConversionServerPolicy | 1886 |
| Utilizzo di questa politica | 1887 |
| Dettagli della politica | 1887 |
| Versione della politica | 1887 |
| Documento di policy JSON | 1887 |
| Ulteriori informazioni | 1888 |

| | |
|---|------|
| AWSElasticDisasterRecoveryCrossAccountReplicationPolicy | 1888 |
| Utilizzo di questa politica | 1888 |
| Dettagli della politica | 1888 |
| Versione della politica | 1888 |
| Documento di policy JSON | 1889 |
| Ulteriori informazioni | 1889 |
| AWSElasticDisasterRecoveryEc2InstancePolicy | 1890 |
| Utilizzo di questa politica | 1890 |
| Dettagli della politica | 1890 |
| Versione della politica | 1890 |
| Documento di policy JSON | 1890 |
| Ulteriori informazioni | 1892 |
| AWSElasticDisasterRecoveryFailbackInstallationPolicy | 1893 |
| Utilizzo di questa politica | 1893 |
| Dettagli della politica | 1893 |
| Versione della politica | 1893 |
| Documento di policy JSON | 1893 |
| Ulteriori informazioni | 1894 |
| AWSElasticDisasterRecoveryFailbackPolicy | 1894 |
| Utilizzo di questa politica | 1895 |
| Dettagli della politica | 1895 |
| Versione della politica | 1895 |
| Documento di policy JSON | 1895 |
| Ulteriori informazioni | 1896 |
| AWSElasticDisasterRecoveryLaunchActionsPolicy | 1897 |
| Utilizzo di questa politica | 1897 |
| Dettagli della politica | 1897 |
| Versione della politica | 1897 |
| Documento di policy JSON | 1897 |
| Ulteriori informazioni | 1903 |
| AWSElasticDisasterRecoveryNetworkReplicationPolicy | 1903 |
| Utilizzo di questa politica | 1904 |
| Dettagli della politica | 1904 |
| Versione della politica | 1904 |
| Documento di policy JSON | 1904 |
| Ulteriori informazioni | 1905 |

| | |
|---|------|
| AWSElasticDisasterRecoveryReadOnlyAccess | 1905 |
| Utilizzo di questa politica | 1905 |
| Dettagli della politica | 1905 |
| Versione della politica | 1906 |
| Documento di policy JSON | 1906 |
| Ulteriori informazioni | 1908 |
| AWSElasticDisasterRecoveryRecoveryInstancePolicy | 1908 |
| Utilizzo di questa politica | 1908 |
| Dettagli della politica | 1908 |
| Versione della politica | 1909 |
| Documento di policy JSON | 1909 |
| Ulteriori informazioni | 1911 |
| AWSElasticDisasterRecoveryReplicationServerPolicy | 1912 |
| Utilizzo di questa politica | 1912 |
| Dettagli della politica | 1912 |
| Versione della politica | 1912 |
| Documento di policy JSON | 1912 |
| Ulteriori informazioni | 1915 |
| AWSElasticDisasterRecoveryServiceRolePolicy | 1915 |
| Utilizzo di questa politica | 1915 |
| Dettagli della politica | 1915 |
| Versione della politica | 1915 |
| Documento di policy JSON | 1916 |
| Ulteriori informazioni | 1924 |
| AWSElasticDisasterRecoveryStagingAccountPolicy | 1924 |
| Utilizzo di questa politica | 1924 |
| Dettagli della politica | 1924 |
| Versione della politica | 1925 |
| Documento di policy JSON | 1925 |
| Ulteriori informazioni | 1926 |
| AWSElasticDisasterRecoveryStagingAccountPolicy_v2 | 1926 |
| Utilizzo di questa politica | 1926 |
| Dettagli della politica | 1926 |
| Versione della politica | 1927 |
| Documento di policy JSON | 1927 |
| Ulteriori informazioni | 1928 |

| | |
|---|------|
| AWSElasticLoadBalancingClassicServiceRolePolicy | 1928 |
| Utilizzo di questa politica | 1928 |
| Dettagli della politica | 1928 |
| Versione della politica | 1929 |
| Documento di policy JSON | 1929 |
| Ulteriori informazioni | 1930 |
| AWSElasticLoadBalancingServiceRolePolicy | 1930 |
| Utilizzo di questa politica | 1930 |
| Dettagli della politica | 1930 |
| Versione della politica | 1930 |
| Documento di policy JSON | 1930 |
| Ulteriori informazioni | 1932 |
| AWSElementalMediaConvertFullAccess | 1932 |
| Utilizzo di questa politica | 1932 |
| Dettagli della politica | 1932 |
| Versione della politica | 1932 |
| Documento di policy JSON | 1932 |
| Ulteriori informazioni | 1933 |
| AWSElementalMediaConvertReadOnly | 1933 |
| Utilizzo di questa politica | 1934 |
| Dettagli della politica | 1934 |
| Versione della politica | 1934 |
| Documento di policy JSON | 1934 |
| Ulteriori informazioni | 1935 |
| AWSElementalMediaLiveFullAccess | 1935 |
| Utilizzo di questa politica | 1935 |
| Dettagli della politica | 1935 |
| Versione della politica | 1935 |
| Documento di policy JSON | 1935 |
| Ulteriori informazioni | 1936 |
| AWSElementalMediaLiveReadOnly | 1936 |
| Utilizzo di questa politica | 1936 |
| Dettagli della politica | 1936 |
| Versione della politica | 1936 |
| Documento di policy JSON | 1937 |
| Ulteriori informazioni | 1937 |

| | |
|--|------|
| AWSElementalMediaPackageFullAccess | 1937 |
| Utilizzo di questa politica | 1937 |
| Dettagli della politica | 1937 |
| Versione della politica | 1938 |
| Documento di policy JSON | 1938 |
| Ulteriori informazioni | 1938 |
| AWSElementalMediaPackageReadOnly | 1938 |
| Utilizzo di questa politica | 1938 |
| Dettagli della politica | 1938 |
| Versione della politica | 1939 |
| Documento di policy JSON | 1939 |
| Ulteriori informazioni | 1939 |
| AWSElementalMediaPackageV2FullAccess | 1939 |
| Utilizzo di questa politica | 1940 |
| Dettagli della politica | 1940 |
| Versione della politica | 1940 |
| Documento di policy JSON | 1940 |
| Ulteriori informazioni | 1940 |
| AWSElementalMediaPackageV2ReadOnly | 1941 |
| Utilizzo di questa politica | 1941 |
| Dettagli della politica | 1941 |
| Versione della politica | 1941 |
| Documento di policy JSON | 1941 |
| Ulteriori informazioni | 1942 |
| AWSElementalMediaStoreFullAccess | 1942 |
| Utilizzo di questa politica | 1942 |
| Dettagli della politica | 1942 |
| Versione della politica | 1942 |
| Documento di policy JSON | 1942 |
| Ulteriori informazioni | 1943 |
| AWSElementalMediaStoreReadOnly | 1943 |
| Utilizzo di questa politica | 1943 |
| Dettagli della politica | 1943 |
| Versione della politica | 1944 |
| Documento di policy JSON | 1944 |
| Ulteriori informazioni | 1944 |

| | |
|---|------|
| AWSElementalMediaTailorFullAccess | 1944 |
| Utilizzo di questa politica | 1945 |
| Dettagli della politica | 1945 |
| Versione della politica | 1945 |
| Documento di policy JSON | 1945 |
| Ulteriori informazioni | 1945 |
| AWSElementalMediaTailorReadOnly | 1946 |
| Utilizzo di questa politica | 1946 |
| Dettagli della politica | 1946 |
| Versione della politica | 1946 |
| Documento di policy JSON | 1946 |
| Ulteriori informazioni | 1947 |
| AWSEnhancedClassicNetworkingMangementPolicy | 1947 |
| Utilizzo di questa politica | 1947 |
| Dettagli della politica | 1947 |
| Versione della politica | 1947 |
| Documento di policy JSON | 1947 |
| Ulteriori informazioni | 1948 |
| AWSEntityResolutionConsoleFullAccess | 1948 |
| Utilizzo di questa politica | 1948 |
| Dettagli della politica | 1948 |
| Versione della politica | 1948 |
| Documento di policy JSON | 1949 |
| Ulteriori informazioni | 1951 |
| AWSEntityResolutionConsoleReadOnlyAccess | 1952 |
| Utilizzo di questa politica | 1952 |
| Dettagli della politica | 1952 |
| Versione della politica | 1952 |
| Documento di policy JSON | 1952 |
| Ulteriori informazioni | 1953 |
| AWSFaultInjectionSimulatorEC2Access | 1953 |
| Utilizzo di questa politica | 1953 |
| Dettagli della politica | 1953 |
| Versione della politica | 1953 |
| Documento di policy JSON | 1954 |
| Ulteriori informazioni | 1955 |

| | |
|---|------|
| AWSFaultInjectionSimulatorECSAccess | 1955 |
| Utilizzo di questa politica | 1955 |
| Dettagli della politica | 1956 |
| Versione della politica | 1956 |
| Documento di policy JSON | 1956 |
| Ulteriori informazioni | 1958 |
| AWSFaultInjectionSimulatorEKSAccess | 1958 |
| Utilizzo di questa politica | 1958 |
| Dettagli della politica | 1958 |
| Versione della politica | 1958 |
| Documento di policy JSON | 1959 |
| Ulteriori informazioni | 1960 |
| AWSFaultInjectionSimulatorNetworkAccess | 1960 |
| Utilizzo di questa politica | 1960 |
| Dettagli della politica | 1960 |
| Versione della politica | 1960 |
| Documento di policy JSON | 1961 |
| Ulteriori informazioni | 1968 |
| AWSFaultInjectionSimulatorRDSAccess | 1968 |
| Utilizzo di questa politica | 1968 |
| Dettagli della politica | 1968 |
| Versione della politica | 1968 |
| Documento di policy JSON | 1968 |
| Ulteriori informazioni | 1970 |
| AWSFaultInjectionSimulatorSSMAccess | 1970 |
| Utilizzo di questa politica | 1970 |
| Dettagli della politica | 1970 |
| Versione della politica | 1970 |
| Documento di policy JSON | 1970 |
| Ulteriori informazioni | 1972 |
| AWSFinSpaceServiceRolePolicy | 1972 |
| Utilizzo di questa politica | 1972 |
| Dettagli della politica | 1972 |
| Versione della politica | 1972 |
| Documento di policy JSON | 1973 |
| Ulteriori informazioni | 1973 |

| | |
|-------------------------------------|------|
| AWSFMAdminFullAccess | 1973 |
| Utilizzo di questa politica | 1973 |
| Dettagli della politica | 1974 |
| Versione della politica | 1974 |
| Documento di policy JSON | 1974 |
| Ulteriori informazioni | 1976 |
| AWSFMAdminReadOnlyAccess | 1976 |
| Utilizzo di questa politica | 1976 |
| Dettagli della politica | 1976 |
| Versione della politica | 1976 |
| Documento di policy JSON | 1977 |
| Ulteriori informazioni | 1978 |
| AWSFMMemberReadOnlyAccess | 1978 |
| Utilizzo di questa politica | 1979 |
| Dettagli della politica | 1979 |
| Versione della politica | 1979 |
| Documento di policy JSON | 1979 |
| Ulteriori informazioni | 1980 |
| AWSForWordPressPluginPolicy | 1980 |
| Utilizzo di questa politica | 1980 |
| Dettagli della politica | 1980 |
| Versione della politica | 1980 |
| Documento di policy JSON | 1980 |
| Ulteriori informazioni | 1982 |
| AWSGitSyncServiceRolePolicy | 1982 |
| Utilizzo di questa politica | 1983 |
| Dettagli della politica | 1983 |
| Versione della politica | 1983 |
| Documento di policy JSON | 1983 |
| Ulteriori informazioni | 1984 |
| AWSGlobalAcceleratorSLRPolicy | 1984 |
| Utilizzo di questa politica | 1984 |
| Dettagli della politica | 1984 |
| Versione della politica | 1984 |
| Documento di policy JSON | 1985 |
| Ulteriori informazioni | 1986 |

| | |
|---|------|
| AWSGlueConsoleFullAccess | 1986 |
| Utilizzo di questa politica | 1986 |
| Dettagli della politica | 1987 |
| Versione della politica | 1987 |
| Documento di policy JSON | 1987 |
| Ulteriori informazioni | 1991 |
| AWSGlueConsoleSageMakerNotebookFullAccess | 1991 |
| Utilizzo di questa politica | 1991 |
| Dettagli della politica | 1992 |
| Versione della politica | 1992 |
| Documento di policy JSON | 1992 |
| Ulteriori informazioni | 1997 |
| AwsGlueDataBrewFullAccessPolicy | 1997 |
| Utilizzo di questa politica | 1998 |
| Dettagli della politica | 1998 |
| Versione della politica | 1998 |
| Documento di policy JSON | 1998 |
| Ulteriori informazioni | 2003 |
| AWSGlueDataBrewServiceRole | 2003 |
| Utilizzo di questa politica | 2004 |
| Dettagli della politica | 2004 |
| Versione della politica | 2004 |
| Documento di policy JSON | 2004 |
| Ulteriori informazioni | 2007 |
| AWSGlueSchemaRegistryFullAccess | 2007 |
| Utilizzo di questa politica | 2007 |
| Dettagli della politica | 2007 |
| Versione della politica | 2007 |
| Documento di policy JSON | 2008 |
| Ulteriori informazioni | 2009 |
| AWSGlueSchemaRegistryReadOnlyAccess | 2009 |
| Utilizzo di questa politica | 2009 |
| Dettagli della politica | 2009 |
| Versione della politica | 2009 |
| Documento di policy JSON | 2010 |
| Ulteriori informazioni | 2010 |

| | |
|---|------|
| AWSGlueServiceNotebookRole | 2011 |
| Utilizzo di questa politica | 2011 |
| Dettagli della politica | 2011 |
| Versione della politica | 2011 |
| Documento di policy JSON | 2011 |
| Ulteriori informazioni | 2014 |
| AWSGlueServiceRole | 2014 |
| Utilizzo di questa politica | 2014 |
| Dettagli della politica | 2014 |
| Versione della politica | 2014 |
| Documento di policy JSON | 2014 |
| Ulteriori informazioni | 2017 |
| AwsGlueSessionUserRestrictedNotebookPolicy | 2017 |
| Utilizzo di questa politica | 2017 |
| Dettagli della politica | 2017 |
| Versione della politica | 2017 |
| Documento di policy JSON | 2018 |
| Ulteriori informazioni | 2020 |
| AwsGlueSessionUserRestrictedNotebookServiceRole | 2020 |
| Utilizzo di questa politica | 2021 |
| Dettagli della politica | 2021 |
| Versione della politica | 2021 |
| Documento di policy JSON | 2021 |
| Ulteriori informazioni | 2025 |
| AwsGlueSessionUserRestrictedPolicy | 2025 |
| Utilizzo di questa politica | 2025 |
| Dettagli della politica | 2025 |
| Versione della politica | 2025 |
| Documento di policy JSON | 2026 |
| Ulteriori informazioni | 2028 |
| AwsGlueSessionUserRestrictedServiceRole | 2028 |
| Utilizzo di questa politica | 2028 |
| Dettagli della politica | 2029 |
| Versione della politica | 2029 |
| Documento di policy JSON | 2029 |
| Ulteriori informazioni | 2033 |

| | |
|---|------|
| AWSGrafanaAccountAdministrator | 2033 |
| Utilizzo di questa politica | 2033 |
| Dettagli della politica | 2034 |
| Versione della politica | 2034 |
| Documento di policy JSON | 2034 |
| Ulteriori informazioni | 2035 |
| AWSGrafanaConsoleReadOnlyAccess | 2035 |
| Utilizzo di questa politica | 2035 |
| Dettagli della politica | 2035 |
| Versione della politica | 2036 |
| Documento di policy JSON | 2036 |
| Ulteriori informazioni | 2036 |
| AWSGrafanaWorkspacePermissionManagement | 2036 |
| Utilizzo di questa politica | 2037 |
| Dettagli della politica | 2037 |
| Versione della politica | 2037 |
| Documento di policy JSON | 2037 |
| Ulteriori informazioni | 2038 |
| AWSGrafanaWorkspacePermissionManagementV2 | 2038 |
| Utilizzo di questa politica | 2038 |
| Dettagli della politica | 2038 |
| Versione della politica | 2039 |
| Documento di policy JSON | 2039 |
| Ulteriori informazioni | 2040 |
| AWSGreengrassFullAccess | 2040 |
| Utilizzo di questa politica | 2040 |
| Dettagli della politica | 2040 |
| Versione della politica | 2040 |
| Documento di policy JSON | 2041 |
| Ulteriori informazioni | 2041 |
| AWSGreengrassReadOnlyAccess | 2041 |
| Utilizzo di questa politica | 2041 |
| Dettagli della politica | 2041 |
| Versione della politica | 2042 |
| Documento di policy JSON | 2042 |
| Ulteriori informazioni | 2042 |

| | |
|---|------|
| AWSGreengrassResourceAccessRolePolicy | 2042 |
| Utilizzo di questa politica | 2043 |
| Dettagli della politica | 2043 |
| Versione della politica | 2043 |
| Documento di policy JSON | 2043 |
| Ulteriori informazioni | 2045 |
| AWSGroundStationAgentInstancePolicy | 2046 |
| Utilizzo di questa politica | 2046 |
| Dettagli della politica | 2046 |
| Versione della politica | 2046 |
| Documento di policy JSON | 2046 |
| Ulteriori informazioni | 2047 |
| AWSHealth_EventProcessorServiceRolePolicy | 2047 |
| Utilizzo di questa politica | 2047 |
| Dettagli della politica | 2047 |
| Versione della politica | 2047 |
| Documento di policy JSON | 2048 |
| Ulteriori informazioni | 2048 |
| AWSHealthFullAccess | 2048 |
| Utilizzo di questa politica | 2049 |
| Dettagli della politica | 2049 |
| Versione della politica | 2049 |
| Documento di policy JSON | 2049 |
| Ulteriori informazioni | 2050 |
| AWSHealthImagingFullAccess | 2050 |
| Utilizzo di questa politica | 2050 |
| Dettagli della politica | 2051 |
| Versione della politica | 2051 |
| Documento di policy JSON | 2051 |
| Ulteriori informazioni | 2052 |
| AWSHealthImagingReadOnlyAccess | 2052 |
| Utilizzo di questa politica | 2052 |
| Dettagli della politica | 2052 |
| Versione della politica | 2052 |
| Documento di policy JSON | 2052 |
| Ulteriori informazioni | 2053 |

| | |
|---|------|
| AWSIAMIdentityCenterAllowListForIdentityContext | 2053 |
| Utilizzo di questa politica | 2053 |
| Dettagli della politica | 2054 |
| Versione della politica | 2054 |
| Documento di policy JSON | 2054 |
| Ulteriori informazioni | 2057 |
| AWSIdentitySyncFullAccess | 2057 |
| Utilizzo di questa politica | 2057 |
| Dettagli della politica | 2057 |
| Versione della politica | 2057 |
| Documento di policy JSON | 2058 |
| Ulteriori informazioni | 2058 |
| AWSIdentitySyncReadOnlyAccess | 2059 |
| Utilizzo di questa politica | 2059 |
| Dettagli della politica | 2059 |
| Versione della politica | 2059 |
| Documento di policy JSON | 2059 |
| Ulteriori informazioni | 2060 |
| AWSImageBuilderFullAccess | 2060 |
| Utilizzo di questa politica | 2060 |
| Dettagli della politica | 2060 |
| Versione della politica | 2060 |
| Documento di policy JSON | 2061 |
| Ulteriori informazioni | 2063 |
| AWSImageBuilderReadOnlyAccess | 2063 |
| Utilizzo di questa politica | 2064 |
| Dettagli della politica | 2064 |
| Versione della politica | 2064 |
| Documento di policy JSON | 2064 |
| Ulteriori informazioni | 2065 |
| AWSImportExportFullAccess | 2065 |
| Utilizzo di questa politica | 2065 |
| Dettagli della politica | 2065 |
| Versione della politica | 2065 |
| Documento di policy JSON | 2066 |
| Ulteriori informazioni | 2066 |

| | |
|---|------|
| AWSImportExportReadOnlyAccess | 2066 |
| Utilizzo di questa politica | 2066 |
| Dettagli della politica | 2066 |
| Versione della politica | 2067 |
| Documento di policy JSON | 2067 |
| Ulteriori informazioni | 2067 |
| AWSIncidentManagerIncidentAccessServiceRolePolicy | 2067 |
| Utilizzo di questa politica | 2068 |
| Dettagli della politica | 2068 |
| Versione della politica | 2068 |
| Documento di policy JSON | 2068 |
| Ulteriori informazioni | 2069 |
| AWSIncidentManagerResolverAccess | 2069 |
| Utilizzo di questa politica | 2069 |
| Dettagli della politica | 2069 |
| Versione della politica | 2069 |
| Documento di policy JSON | 2070 |
| Ulteriori informazioni | 2071 |
| AWSIncidentManagerServiceRolePolicy | 2071 |
| Utilizzo di questa politica | 2071 |
| Dettagli della politica | 2071 |
| Versione della politica | 2071 |
| Documento di policy JSON | 2072 |
| Ulteriori informazioni | 2073 |
| AWSIoT1ClickFullAccess | 2073 |
| Utilizzo di questa politica | 2073 |
| Dettagli della politica | 2073 |
| Versione della politica | 2073 |
| Documento di policy JSON | 2073 |
| Ulteriori informazioni | 2074 |
| AWSIoT1ClickReadOnlyAccess | 2074 |
| Utilizzo di questa politica | 2074 |
| Dettagli della politica | 2074 |
| Versione della politica | 2074 |
| Documento di policy JSON | 2075 |
| Ulteriori informazioni | 2075 |

| | |
|---|------|
| AWSIoTAnalyticsFullAccess | 2075 |
| Utilizzo di questa politica | 2075 |
| Dettagli della politica | 2076 |
| Versione della politica | 2076 |
| Documento di policy JSON | 2076 |
| Ulteriori informazioni | 2076 |
| AWSIoTAnalyticsReadOnlyAccess | 2077 |
| Utilizzo di questa politica | 2077 |
| Dettagli della politica | 2077 |
| Versione della politica | 2077 |
| Documento di policy JSON | 2077 |
| Ulteriori informazioni | 2078 |
| AWSIoTConfigAccess | 2078 |
| Utilizzo di questa politica | 2078 |
| Dettagli della politica | 2078 |
| Versione della politica | 2078 |
| Documento di policy JSON | 2079 |
| Ulteriori informazioni | 2082 |
| AWSIoTConfigReadOnlyAccess | 2083 |
| Utilizzo di questa politica | 2083 |
| Dettagli della politica | 2083 |
| Versione della politica | 2083 |
| Documento di policy JSON | 2083 |
| Ulteriori informazioni | 2085 |
| AWSIoTDataAccess | 2085 |
| Utilizzo di questa politica | 2085 |
| Dettagli della politica | 2086 |
| Versione della politica | 2086 |
| Documento di policy JSON | 2086 |
| Ulteriori informazioni | 2086 |
| AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction | 2087 |
| Utilizzo di questa politica | 2087 |
| Dettagli della politica | 2087 |
| Versione della politica | 2087 |
| Documento di policy JSON | 2087 |
| Ulteriori informazioni | 2088 |

| | |
|--|------|
| AWSIoTDeviceDefenderAudit | 2088 |
| Utilizzo di questa politica | 2088 |
| Dettagli della politica | 2088 |
| Versione della politica | 2089 |
| Documento di policy JSON | 2089 |
| Ulteriori informazioni | 2090 |
| AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction | 2090 |
| Utilizzo di questa politica | 2090 |
| Dettagli della politica | 2090 |
| Versione della politica | 2090 |
| Documento di policy JSON | 2091 |
| Ulteriori informazioni | 2091 |
| AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction | 2092 |
| Utilizzo di questa politica | 2092 |
| Dettagli della politica | 2092 |
| Versione della politica | 2092 |
| Documento di policy JSON | 2092 |
| Ulteriori informazioni | 2093 |
| AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction | 2093 |
| Utilizzo di questa politica | 2093 |
| Dettagli della politica | 2093 |
| Versione della politica | 2094 |
| Documento di policy JSON | 2094 |
| Ulteriori informazioni | 2094 |
| AWSIoTDeviceDefenderUpdateCACertMitigationAction | 2094 |
| Utilizzo di questa politica | 2095 |
| Dettagli della politica | 2095 |
| Versione della politica | 2095 |
| Documento di policy JSON | 2095 |
| Ulteriori informazioni | 2096 |
| AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction | 2096 |
| Utilizzo di questa politica | 2096 |
| Dettagli della politica | 2096 |
| Versione della politica | 2096 |
| Documento di policy JSON | 2097 |
| Ulteriori informazioni | 2097 |

| | |
|---|------|
| AWSIoTDeviceTesterForFreeRTOSFullAccess | 2097 |
| Utilizzo di questa politica | 2097 |
| Dettagli della politica | 2097 |
| Versione della politica | 2098 |
| Documento di policy JSON | 2098 |
| Ulteriori informazioni | 2104 |
| AWSIoTDeviceTesterForGreengrassFullAccess | 2104 |
| Utilizzo di questa politica | 2104 |
| Dettagli della politica | 2104 |
| Versione della politica | 2105 |
| Documento di policy JSON | 2105 |
| Ulteriori informazioni | 2108 |
| AWSIoTEventsFullAccess | 2108 |
| Utilizzo di questa politica | 2108 |
| Dettagli della politica | 2108 |
| Versione della politica | 2108 |
| Documento di policy JSON | 2109 |
| Ulteriori informazioni | 2109 |
| AWSIoTEventsReadOnlyAccess | 2109 |
| Utilizzo di questa politica | 2109 |
| Dettagli della politica | 2109 |
| Versione della politica | 2110 |
| Documento di policy JSON | 2110 |
| Ulteriori informazioni | 2110 |
| AWSIoTFleetHubFederationAccess | 2110 |
| Utilizzo di questa politica | 2110 |
| Dettagli della politica | 2111 |
| Versione della politica | 2111 |
| Documento di policy JSON | 2111 |
| Ulteriori informazioni | 2113 |
| AWSIoTFleetwiseServiceRolePolicy | 2113 |
| Utilizzo di questa politica | 2113 |
| Dettagli della politica | 2113 |
| Versione della politica | 2113 |
| Documento di policy JSON | 2114 |
| Ulteriori informazioni | 2114 |

| | |
|---|------|
| AWSIoTFullAccess | 2114 |
| Utilizzo di questa politica | 2115 |
| Dettagli della politica | 2115 |
| Versione della politica | 2115 |
| Documento di policy JSON | 2115 |
| Ulteriori informazioni | 2115 |
| AWSIoTLogging | 2116 |
| Utilizzo di questa politica | 2116 |
| Dettagli della politica | 2116 |
| Versione della politica | 2116 |
| Documento di policy JSON | 2116 |
| Ulteriori informazioni | 2117 |
| AWSIoTOTAUpdate | 2117 |
| Utilizzo di questa politica | 2117 |
| Dettagli della politica | 2117 |
| Versione della politica | 2118 |
| Documento di policy JSON | 2118 |
| Ulteriori informazioni | 2118 |
| AWSIoTRoboRunnerFullAccess | 2118 |
| Utilizzo di questa politica | 2119 |
| Dettagli della politica | 2119 |
| Versione della politica | 2119 |
| Documento di policy JSON | 2119 |
| Ulteriori informazioni | 2120 |
| AWSIoTRoboRunnerReadOnly | 2120 |
| Utilizzo di questa politica | 2120 |
| Dettagli della politica | 2120 |
| Versione della politica | 2120 |
| Documento di policy JSON | 2121 |
| Ulteriori informazioni | 2121 |
| AWSIoTRoboRunnerServiceRolePolicy | 2121 |
| Utilizzo di questa politica | 2122 |
| Dettagli della politica | 2122 |
| Versione della politica | 2122 |
| Documento di policy JSON | 2122 |
| Ulteriori informazioni | 2123 |

| | |
|--|------|
| AWSIoTRuleActions | 2123 |
| Utilizzo di questa politica | 2123 |
| Dettagli della politica | 2123 |
| Versione della politica | 2123 |
| Documento di policy JSON | 2123 |
| Ulteriori informazioni | 2124 |
| AWSIoTSiteWiseConsoleFullAccess | 2124 |
| Utilizzo di questa politica | 2124 |
| Dettagli della politica | 2125 |
| Versione della politica | 2125 |
| Documento di policy JSON | 2125 |
| Ulteriori informazioni | 2127 |
| AWSIoTSiteWiseFullAccess | 2127 |
| Utilizzo di questa politica | 2127 |
| Dettagli della politica | 2127 |
| Versione della politica | 2128 |
| Documento di policy JSON | 2128 |
| Ulteriori informazioni | 2128 |
| AWSIoTSiteWiseMonitorPortalAccess | 2128 |
| Utilizzo di questa politica | 2129 |
| Dettagli della politica | 2129 |
| Versione della politica | 2129 |
| Documento di policy JSON | 2129 |
| Ulteriori informazioni | 2130 |
| AWSIoTSiteWiseMonitorServiceRolePolicy | 2130 |
| Utilizzo di questa politica | 2131 |
| Dettagli della politica | 2131 |
| Versione della politica | 2131 |
| Documento di policy JSON | 2131 |
| Ulteriori informazioni | 2132 |
| AWSIoTSiteWiseReadOnlyAccess | 2132 |
| Utilizzo di questa politica | 2132 |
| Dettagli della politica | 2132 |
| Versione della politica | 2133 |
| Documento di policy JSON | 2133 |
| Ulteriori informazioni | 2133 |

| | |
|--|------|
| AWSIoTThingsRegistration | 2134 |
| Utilizzo di questa politica | 2134 |
| Dettagli della politica | 2134 |
| Versione della politica | 2134 |
| Documento di policy JSON | 2134 |
| Ulteriori informazioni | 2135 |
| AWSIoTTwinMakerServiceRolePolicy | 2136 |
| Utilizzo di questa politica | 2136 |
| Dettagli della politica | 2136 |
| Versione della politica | 2136 |
| Documento di policy JSON | 2136 |
| Ulteriori informazioni | 2138 |
| AWSIoTWirelessDataAccess | 2138 |
| Utilizzo di questa politica | 2138 |
| Dettagli della politica | 2138 |
| Versione della politica | 2138 |
| Documento di policy JSON | 2139 |
| Ulteriori informazioni | 2139 |
| AWSIoTWirelessFullAccess | 2139 |
| Utilizzo di questa politica | 2139 |
| Dettagli della politica | 2139 |
| Versione della politica | 2140 |
| Documento di policy JSON | 2140 |
| Ulteriori informazioni | 2140 |
| AWSIoTWirelessFullPublishAccess | 2140 |
| Utilizzo di questa politica | 2141 |
| Dettagli della politica | 2141 |
| Versione della politica | 2141 |
| Documento di policy JSON | 2141 |
| Ulteriori informazioni | 2141 |
| AWSIoTWirelessGatewayCertManager | 2142 |
| Utilizzo di questa politica | 2142 |
| Dettagli della politica | 2142 |
| Versione della politica | 2142 |
| Documento di policy JSON | 2142 |
| Ulteriori informazioni | 2143 |

| | |
|--|------|
| AWSIoTWirelessLogging | 2143 |
| Utilizzo di questa politica | 2143 |
| Dettagli della politica | 2143 |
| Versione della politica | 2143 |
| Documento di policy JSON | 2144 |
| Ulteriori informazioni | 2144 |
| AWSIoTWirelessReadOnlyAccess | 2144 |
| Utilizzo di questa politica | 2144 |
| Dettagli della politica | 2145 |
| Versione della politica | 2145 |
| Documento di policy JSON | 2145 |
| Ulteriori informazioni | 2145 |
| AWSIPAMServiceRolePolicy | 2146 |
| Utilizzo di questa politica | 2146 |
| Dettagli della politica | 2146 |
| Versione della politica | 2146 |
| Documento di policy JSON | 2146 |
| Ulteriori informazioni | 2147 |
| AWSIQContractServiceRolePolicy | 2147 |
| Utilizzo di questa politica | 2148 |
| Dettagli della politica | 2148 |
| Versione della politica | 2148 |
| Documento di policy JSON | 2148 |
| Ulteriori informazioni | 2149 |
| AWSIQFullAccess | 2149 |
| Utilizzo di questa politica | 2149 |
| Dettagli della politica | 2149 |
| Versione della politica | 2149 |
| Documento di policy JSON | 2149 |
| Ulteriori informazioni | 2150 |
| AWSIQPermissionServiceRolePolicy | 2150 |
| Utilizzo di questa politica | 2150 |
| Dettagli della politica | 2151 |
| Versione della politica | 2151 |
| Documento di policy JSON | 2151 |
| Ulteriori informazioni | 2152 |

| | |
|---|------|
| AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy | 2152 |
| Utilizzo di questa politica | 2152 |
| Dettagli della politica | 2152 |
| Versione della politica | 2153 |
| Documento di policy JSON | 2153 |
| Ulteriori informazioni | 2153 |
| AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy | 2153 |
| Utilizzo di questa politica | 2154 |
| Dettagli della politica | 2154 |
| Versione della politica | 2154 |
| Documento di policy JSON | 2154 |
| Ulteriori informazioni | 2155 |
| AWSKeyManagementServicePowerUser | 2155 |
| Utilizzo di questa politica | 2155 |
| Dettagli della politica | 2155 |
| Versione della politica | 2155 |
| Documento di policy JSON | 2155 |
| Ulteriori informazioni | 2156 |
| AWSLakeFormationCrossAccountManager | 2156 |
| Utilizzo di questa politica | 2156 |
| Dettagli della politica | 2156 |
| Versione della politica | 2157 |
| Documento di policy JSON | 2157 |
| Ulteriori informazioni | 2159 |
| AWSLakeFormationDataAdmin | 2159 |
| Utilizzo di questa politica | 2159 |
| Dettagli della politica | 2159 |
| Versione della politica | 2159 |
| Documento di policy JSON | 2160 |
| Ulteriori informazioni | 2161 |
| AWSLambda_FullAccess | 2161 |
| Utilizzo di questa politica | 2161 |
| Dettagli della politica | 2161 |
| Versione della politica | 2162 |
| Documento di policy JSON | 2162 |
| Ulteriori informazioni | 2163 |

| | |
|--------------------------------------|------|
| AWSLambda_ReadOnlyAccess | 2163 |
| Utilizzo di questa politica | 2163 |
| Dettagli della politica | 2164 |
| Versione della politica | 2164 |
| Documento di policy JSON | 2164 |
| Ulteriori informazioni | 2165 |
| AWSLambdaBasicExecutionRole | 2165 |
| Utilizzo di questa politica | 2166 |
| Dettagli della politica | 2166 |
| Versione della politica | 2166 |
| Documento di policy JSON | 2166 |
| Ulteriori informazioni | 2166 |
| AWSLambdaDynamoDBExecutionRole | 2167 |
| Utilizzo di questa politica | 2167 |
| Dettagli della politica | 2167 |
| Versione della politica | 2167 |
| Documento di policy JSON | 2167 |
| Ulteriori informazioni | 2168 |
| AWSLambdaENIManagementAccess | 2168 |
| Utilizzo di questa politica | 2168 |
| Dettagli della politica | 2168 |
| Versione della politica | 2169 |
| Documento di policy JSON | 2169 |
| Ulteriori informazioni | 2169 |
| AWSLambdaExecute | 2169 |
| Utilizzo di questa politica | 2170 |
| Dettagli della politica | 2170 |
| Versione della politica | 2170 |
| Documento di policy JSON | 2170 |
| Ulteriori informazioni | 2171 |
| AWSLambdaFullAccess | 2171 |
| Utilizzo di questa politica | 2171 |
| Dettagli della politica | 2171 |
| Versione della politica | 2171 |
| Documento di policy JSON | 2172 |
| Ulteriori informazioni | 2173 |

| | |
|--------------------------------------|------|
| AWSLambdaInvocation-DynamoDB | 2173 |
| Utilizzo di questa politica | 2173 |
| Dettagli della politica | 2174 |
| Versione della politica | 2174 |
| Documento di policy JSON | 2174 |
| Ulteriori informazioni | 2175 |
| AWSLambdaKinesisExecutionRole | 2175 |
| Utilizzo di questa politica | 2175 |
| Dettagli della politica | 2175 |
| Versione della politica | 2175 |
| Documento di policy JSON | 2175 |
| Ulteriori informazioni | 2176 |
| AWSLambdaMSKExecutionRole | 2176 |
| Utilizzo di questa politica | 2176 |
| Dettagli della politica | 2177 |
| Versione della politica | 2177 |
| Documento di policy JSON | 2177 |
| Ulteriori informazioni | 2178 |
| AWSLambdaReplicator | 2178 |
| Utilizzo di questa politica | 2178 |
| Dettagli della politica | 2178 |
| Versione della politica | 2178 |
| Documento di policy JSON | 2178 |
| Ulteriori informazioni | 2180 |
| AWSLambdaRole | 2180 |
| Utilizzo di questa politica | 2180 |
| Dettagli della politica | 2180 |
| Versione della politica | 2180 |
| Documento di policy JSON | 2180 |
| Ulteriori informazioni | 2181 |
| AWSLambdaSQSQueueExecutionRole | 2181 |
| Utilizzo di questa politica | 2181 |
| Dettagli della politica | 2181 |
| Versione della politica | 2181 |
| Documento di policy JSON | 2182 |
| Ulteriori informazioni | 2182 |

| | |
|--|------|
| AWSLambdaVPCLambdaAccessExecutionRole | 2182 |
| Utilizzo di questa politica | 2183 |
| Dettagli della politica | 2183 |
| Versione della politica | 2183 |
| Documento di policy JSON | 2183 |
| Ulteriori informazioni | 2184 |
| AWSLicenseManagerConsumptionPolicy | 2184 |
| Utilizzo di questa politica | 2184 |
| Dettagli della politica | 2184 |
| Versione della politica | 2184 |
| Documento di policy JSON | 2185 |
| Ulteriori informazioni | 2185 |
| AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy | 2185 |
| Utilizzo di questa politica | 2185 |
| Dettagli della politica | 2185 |
| Versione della politica | 2186 |
| Documento di policy JSON | 2186 |
| Ulteriori informazioni | 2187 |
| AWSLicenseManagerMasterAccountRolePolicy | 2187 |
| Utilizzo di questa politica | 2187 |
| Dettagli della politica | 2187 |
| Versione della politica | 2187 |
| Documento di policy JSON | 2188 |
| Ulteriori informazioni | 2192 |
| AWSLicenseManagerMemberAccountRolePolicy | 2193 |
| Utilizzo di questa politica | 2193 |
| Dettagli della politica | 2193 |
| Versione della politica | 2193 |
| Documento di policy JSON | 2193 |
| Ulteriori informazioni | 2194 |
| AWSLicenseManagerServiceRolePolicy | 2194 |
| Utilizzo di questa politica | 2195 |
| Dettagli della politica | 2195 |
| Versione della politica | 2195 |
| Documento di policy JSON | 2195 |
| Ulteriori informazioni | 2198 |

| | |
|--|------|
| AWSLicenseManagerUserSubscriptionsServiceRolePolicy | 2199 |
| Utilizzo di questa politica | 2199 |
| Dettagli della politica | 2199 |
| Versione della politica | 2199 |
| Documento di policy JSON | 2199 |
| Ulteriori informazioni | 2201 |
| AWSM2ServicePolicy | 2201 |
| Utilizzo di questa politica | 2201 |
| Dettagli della politica | 2202 |
| Versione della politica | 2202 |
| Documento di policy JSON | 2202 |
| Ulteriori informazioni | 2203 |
| AWSManagedServices_ContactsServiceRolePolicy | 2203 |
| Utilizzo di questa politica | 2204 |
| Dettagli della politica | 2204 |
| Versione della politica | 2204 |
| Documento di policy JSON | 2204 |
| Ulteriori informazioni | 2205 |
| AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy | 2205 |
| Utilizzo di questa politica | 2205 |
| Dettagli della politica | 2205 |
| Versione della politica | 2206 |
| Documento di policy JSON | 2206 |
| Ulteriori informazioni | 2207 |
| AWSManagedServices_EventsServiceRolePolicy | 2207 |
| Utilizzo di questa politica | 2208 |
| Dettagli della politica | 2208 |
| Versione della politica | 2208 |
| Documento di policy JSON | 2208 |
| Ulteriori informazioni | 2209 |
| AWSManagedServicesDeploymentToolkitPolicy | 2209 |
| Utilizzo di questa politica | 2209 |
| Dettagli della politica | 2209 |
| Versione della politica | 2210 |
| Documento di policy JSON | 2210 |
| Ulteriori informazioni | 2212 |

| | |
|--|------|
| AWSMarketplaceAmiIngestion | 2212 |
| Utilizzo di questa politica | 2212 |
| Dettagli della politica | 2212 |
| Versione della politica | 2212 |
| Documento di policy JSON | 2213 |
| Ulteriori informazioni | 2213 |
| AWSMarketplaceDeploymentServiceRolePolicy | 2214 |
| Utilizzo di questa politica | 2214 |
| Dettagli della politica | 2214 |
| Versione della politica | 2214 |
| Documento di policy JSON | 2214 |
| Ulteriori informazioni | 2216 |
| AWSMarketplaceFullAccess | 2216 |
| Utilizzo di questa politica | 2216 |
| Dettagli della politica | 2216 |
| Versione della politica | 2216 |
| Documento di policy JSON | 2216 |
| Ulteriori informazioni | 2220 |
| AWSMarketplaceGetEntitlements | 2220 |
| Utilizzo di questa politica | 2220 |
| Dettagli della politica | 2220 |
| Versione della politica | 2220 |
| Documento di policy JSON | 2220 |
| Ulteriori informazioni | 2221 |
| AWSMarketplaceImageBuildFullAccess | 2221 |
| Utilizzo di questa politica | 2221 |
| Dettagli della politica | 2221 |
| Versione della politica | 2222 |
| Documento di policy JSON | 2222 |
| Ulteriori informazioni | 2225 |
| AWSMarketplaceLicenseManagementServiceRolePolicy | 2225 |
| Utilizzo di questa politica | 2226 |
| Dettagli della politica | 2226 |
| Versione della politica | 2226 |
| Documento di policy JSON | 2226 |
| Ulteriori informazioni | 2227 |

| | |
|--|------|
| AWSMarketplaceManageSubscriptions | 2227 |
| Utilizzo di questa politica | 2227 |
| Dettagli della politica | 2227 |
| Versione della politica | 2227 |
| Documento di policy JSON | 2228 |
| Ulteriori informazioni | 2228 |
| AWSMarketplaceMeteringFullAccess | 2229 |
| Utilizzo di questa politica | 2229 |
| Dettagli della politica | 2229 |
| Versione della politica | 2229 |
| Documento di policy JSON | 2229 |
| Ulteriori informazioni | 2230 |
| AWSMarketplaceMeteringRegisterUsage | 2230 |
| Utilizzo di questa politica | 2230 |
| Dettagli della politica | 2230 |
| Versione della politica | 2230 |
| Documento di policy JSON | 2230 |
| Ulteriori informazioni | 2231 |
| AWSMarketplaceProcurementSystemAdminFullAccess | 2231 |
| Utilizzo di questa politica | 2231 |
| Dettagli della politica | 2231 |
| Versione della politica | 2232 |
| Documento di policy JSON | 2232 |
| Ulteriori informazioni | 2232 |
| AWSMarketplacePurchaseOrdersServiceRolePolicy | 2232 |
| Utilizzo di questa politica | 2233 |
| Dettagli della politica | 2233 |
| Versione della politica | 2233 |
| Documento di policy JSON | 2233 |
| Ulteriori informazioni | 2234 |
| AWSMarketplaceRead-only | 2234 |
| Utilizzo di questa politica | 2234 |
| Dettagli della politica | 2234 |
| Versione della politica | 2234 |
| Documento di policy JSON | 2234 |
| Ulteriori informazioni | 2236 |

| | |
|--|------|
| AWSMarketplaceResaleAuthorizationServiceRolePolicy | 2236 |
| Utilizzo di questa politica | 2236 |
| Dettagli della politica | 2236 |
| Versione della politica | 2236 |
| Documento di policy JSON | 2237 |
| Ulteriori informazioni | 2239 |
| AWSMarketplaceSellerFullAccess | 2239 |
| Utilizzo di questa politica | 2239 |
| Dettagli della politica | 2239 |
| Versione della politica | 2239 |
| Documento di policy JSON | 2240 |
| Ulteriori informazioni | 2243 |
| AWSMarketplaceSellerProductsFullAccess | 2243 |
| Utilizzo di questa politica | 2243 |
| Dettagli della politica | 2244 |
| Versione della politica | 2244 |
| Documento di policy JSON | 2244 |
| Ulteriori informazioni | 2246 |
| AWSMarketplaceSellerProductsReadOnly | 2246 |
| Utilizzo di questa politica | 2246 |
| Dettagli della politica | 2246 |
| Versione della politica | 2246 |
| Documento di policy JSON | 2247 |
| Ulteriori informazioni | 2247 |
| AWSMediaConnectServicePolicy | 2248 |
| Utilizzo di questa politica | 2248 |
| Dettagli della politica | 2248 |
| Versione della politica | 2248 |
| Documento di policy JSON | 2248 |
| Ulteriori informazioni | 2249 |
| AWSMediaTailorServiceRolePolicy | 2250 |
| Utilizzo di questa politica | 2250 |
| Dettagli della politica | 2250 |
| Versione della politica | 2250 |
| Documento di policy JSON | 2250 |
| Ulteriori informazioni | 2251 |

| | |
|---|------|
| AWSMigrationHubDiscoveryAccess | 2251 |
| Utilizzo di questa politica | 2251 |
| Dettagli della politica | 2251 |
| Versione della politica | 2251 |
| Documento di policy JSON | 2252 |
| Ulteriori informazioni | 2253 |
| AWSMigrationHubDMSAccess | 2253 |
| Utilizzo di questa politica | 2253 |
| Dettagli della politica | 2253 |
| Versione della politica | 2254 |
| Documento di policy JSON | 2254 |
| Ulteriori informazioni | 2255 |
| AWSMigrationHubFullAccess | 2255 |
| Utilizzo di questa politica | 2255 |
| Dettagli della politica | 2255 |
| Versione della politica | 2255 |
| Documento di policy JSON | 2256 |
| Ulteriori informazioni | 2257 |
| AWSMigrationHubOrchestratorConsoleFullAccess | 2257 |
| Utilizzo di questa politica | 2257 |
| Dettagli della politica | 2257 |
| Versione della politica | 2258 |
| Documento di policy JSON | 2258 |
| Ulteriori informazioni | 2261 |
| AWSMigrationHubOrchestratorInstanceRolePolicy | 2261 |
| Utilizzo di questa politica | 2261 |
| Dettagli della politica | 2261 |
| Versione della politica | 2262 |
| Documento di policy JSON | 2262 |
| Ulteriori informazioni | 2262 |
| AWSMigrationHubOrchestratorPlugin | 2263 |
| Utilizzo di questa politica | 2263 |
| Dettagli della politica | 2263 |
| Versione della politica | 2263 |
| Documento di policy JSON | 2263 |
| Ulteriori informazioni | 2265 |

| | |
|--|------|
| AWSMigrationHubOrchestratorServiceRolePolicy | 2265 |
| Utilizzo di questa politica | 2265 |
| Dettagli della politica | 2265 |
| Versione della politica | 2265 |
| Documento di policy JSON | 2266 |
| Ulteriori informazioni | 2269 |
| AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess | 2269 |
| Utilizzo di questa politica | 2270 |
| Dettagli della politica | 2270 |
| Versione della politica | 2270 |
| Documento di policy JSON | 2270 |
| Ulteriori informazioni | 2276 |
| AWSMigrationHubRefactorSpaces-SSMAutomationPolicy | 2276 |
| Utilizzo di questa politica | 2276 |
| Dettagli della politica | 2276 |
| Versione della politica | 2277 |
| Documento di policy JSON | 2277 |
| Ulteriori informazioni | 2278 |
| AWSMigrationHubRefactorSpacesFullAccess | 2278 |
| Utilizzo di questa politica | 2279 |
| Dettagli della politica | 2279 |
| Versione della politica | 2279 |
| Documento di policy JSON | 2279 |
| Ulteriori informazioni | 2286 |
| AWSMigrationHubRefactorSpacesServiceRolePolicy | 2286 |
| Utilizzo di questa politica | 2286 |
| Dettagli della politica | 2286 |
| Versione della politica | 2286 |
| Documento di policy JSON | 2287 |
| Ulteriori informazioni | 2290 |
| AWSMigrationHubSMSAccess | 2290 |
| Utilizzo di questa politica | 2291 |
| Dettagli della politica | 2291 |
| Versione della politica | 2291 |
| Documento di policy JSON | 2291 |
| Ulteriori informazioni | 2292 |

| | |
|--|------|
| AWSMigrationHubStrategyCollector | 2292 |
| Utilizzo di questa politica | 2292 |
| Dettagli della politica | 2293 |
| Versione della politica | 2293 |
| Documento di policy JSON | 2293 |
| Ulteriori informazioni | 2295 |
| AWSMigrationHubStrategyConsoleFullAccess | 2295 |
| Utilizzo di questa politica | 2296 |
| Dettagli della politica | 2296 |
| Versione della politica | 2296 |
| Documento di policy JSON | 2296 |
| Ulteriori informazioni | 2298 |
| AWSMigrationHubStrategyServiceRolePolicy | 2298 |
| Utilizzo di questa politica | 2298 |
| Dettagli della politica | 2298 |
| Versione della politica | 2299 |
| Documento di policy JSON | 2299 |
| Ulteriori informazioni | 2300 |
| AWSMobileHub_FullAccess | 2300 |
| Utilizzo di questa politica | 2300 |
| Dettagli della politica | 2300 |
| Versione della politica | 2300 |
| Documento di policy JSON | 2301 |
| Ulteriori informazioni | 2302 |
| AWSMobileHub_ReadOnly | 2302 |
| Utilizzo di questa politica | 2302 |
| Dettagli della politica | 2303 |
| Versione della politica | 2303 |
| Documento di policy JSON | 2303 |
| Ulteriori informazioni | 2304 |
| AWSMSKReplicatorExecutionRole | 2304 |
| Utilizzo di questa politica | 2304 |
| Dettagli della politica | 2305 |
| Versione della politica | 2305 |
| Documento di policy JSON | 2305 |
| Ulteriori informazioni | 2306 |

| | |
|--|------|
| AWSNetworkFirewallServiceRolePolicy | 2307 |
| Utilizzo di questa politica | 2307 |
| Dettagli della politica | 2307 |
| Versione della politica | 2307 |
| Documento di policy JSON | 2307 |
| Ulteriori informazioni | 2309 |
| AWSNetworkManagerCloudWANServiceRolePolicy | 2309 |
| Utilizzo di questa politica | 2309 |
| Dettagli della politica | 2309 |
| Versione della politica | 2309 |
| Documento di policy JSON | 2310 |
| Ulteriori informazioni | 2310 |
| AWSNetworkManagerFullAccess | 2310 |
| Utilizzo di questa politica | 2310 |
| Dettagli della politica | 2311 |
| Versione della politica | 2311 |
| Documento di policy JSON | 2311 |
| Ulteriori informazioni | 2312 |
| AWSNetworkManagerReadOnlyAccess | 2312 |
| Utilizzo di questa politica | 2312 |
| Dettagli della politica | 2312 |
| Versione della politica | 2312 |
| Documento di policy JSON | 2312 |
| Ulteriori informazioni | 2313 |
| AWSNetworkManagerServiceRolePolicy | 2313 |
| Utilizzo di questa politica | 2313 |
| Dettagli della politica | 2313 |
| Versione della politica | 2314 |
| Documento di policy JSON | 2314 |
| Ulteriori informazioni | 2315 |
| AWSOpsWorks_FullAccess | 2315 |
| Utilizzo di questa politica | 2315 |
| Dettagli della politica | 2315 |
| Versione della politica | 2315 |
| Documento di policy JSON | 2316 |
| Ulteriori informazioni | 2317 |

| | |
|---|------|
| AWSOpsWorksCloudWatchLogs | 2317 |
| Utilizzo di questa politica | 2317 |
| Dettagli della politica | 2317 |
| Versione della politica | 2317 |
| Documento di policy JSON | 2317 |
| Ulteriori informazioni | 2318 |
| AWSOpsWorksCMInstanceProfileRole | 2318 |
| Utilizzo di questa politica | 2318 |
| Dettagli della politica | 2318 |
| Versione della politica | 2319 |
| Documento di policy JSON | 2319 |
| Ulteriori informazioni | 2320 |
| AWSOpsWorksCMServiceRole | 2320 |
| Utilizzo di questa politica | 2320 |
| Dettagli della politica | 2320 |
| Versione della politica | 2320 |
| Documento di policy JSON | 2321 |
| Ulteriori informazioni | 2325 |
| AWSOpsWorksInstanceRegistration | 2325 |
| Utilizzo di questa politica | 2325 |
| Dettagli della politica | 2325 |
| Versione della politica | 2325 |
| Documento di policy JSON | 2326 |
| Ulteriori informazioni | 2326 |
| AWSOpsWorksRegisterCLI_EC2 | 2326 |
| Utilizzo di questa politica | 2326 |
| Dettagli della politica | 2327 |
| Versione della politica | 2327 |
| Documento di policy JSON | 2327 |
| Ulteriori informazioni | 2328 |
| AWSOpsWorksRegisterCLI_OnPremises | 2328 |
| Utilizzo di questa politica | 2328 |
| Dettagli della politica | 2328 |
| Versione della politica | 2328 |
| Documento di policy JSON | 2329 |
| Ulteriori informazioni | 2330 |

| | |
|--|------|
| AWSOrganizationsFullAccess | 2330 |
| Utilizzo di questa politica | 2330 |
| Dettagli della politica | 2331 |
| Versione della politica | 2331 |
| Documento di policy JSON | 2331 |
| Ulteriori informazioni | 2332 |
| AWSOrganizationsReadOnlyAccess | 2332 |
| Utilizzo di questa politica | 2332 |
| Dettagli della politica | 2332 |
| Versione della politica | 2333 |
| Documento di policy JSON | 2333 |
| Ulteriori informazioni | 2333 |
| AWSOrganizationsServiceTrustPolicy | 2334 |
| Utilizzo di questa politica | 2334 |
| Dettagli della politica | 2334 |
| Versione della politica | 2334 |
| Documento di policy JSON | 2334 |
| Ulteriori informazioni | 2335 |
| AWSOutpostsAuthorizeServerPolicy | 2335 |
| Utilizzo di questa politica | 2335 |
| Dettagli della politica | 2335 |
| Versione della politica | 2336 |
| Documento di policy JSON | 2336 |
| Ulteriori informazioni | 2336 |
| AWSOutpostsServiceRolePolicy | 2336 |
| Utilizzo di questa politica | 2337 |
| Dettagli della politica | 2337 |
| Versione della politica | 2337 |
| Documento di policy JSON | 2337 |
| Ulteriori informazioni | 2338 |
| AWSPanoramaApplianceRolePolicy | 2338 |
| Utilizzo di questa politica | 2338 |
| Dettagli della politica | 2338 |
| Versione della politica | 2338 |
| Documento di policy JSON | 2338 |
| Ulteriori informazioni | 2339 |

| | |
|---|------|
| AWSPanoramaApplianceServiceRolePolicy | 2339 |
| Utilizzo di questa politica | 2339 |
| Dettagli della politica | 2339 |
| Versione della politica | 2340 |
| Documento di policy JSON | 2340 |
| Ulteriori informazioni | 2341 |
| AWSPanoramaFullAccess | 2341 |
| Utilizzo di questa politica | 2342 |
| Dettagli della politica | 2342 |
| Versione della politica | 2342 |
| Documento di policy JSON | 2342 |
| Ulteriori informazioni | 2345 |
| AWSPanoramaGreengrassGroupRolePolicy | 2345 |
| Utilizzo di questa politica | 2345 |
| Dettagli della politica | 2345 |
| Versione della politica | 2345 |
| Documento di policy JSON | 2346 |
| Ulteriori informazioni | 2347 |
| AWSPanoramaSageMakerRolePolicy | 2347 |
| Utilizzo di questa politica | 2347 |
| Dettagli della politica | 2347 |
| Versione della politica | 2348 |
| Documento di policy JSON | 2348 |
| Ulteriori informazioni | 2348 |
| AWSPanoramaServiceLinkedRolePolicy | 2348 |
| Utilizzo di questa politica | 2349 |
| Dettagli della politica | 2349 |
| Versione della politica | 2349 |
| Documento di policy JSON | 2349 |
| Ulteriori informazioni | 2352 |
| AWSPanoramaServiceRolePolicy | 2352 |
| Utilizzo di questa politica | 2352 |
| Dettagli della politica | 2352 |
| Versione della politica | 2352 |
| Documento di policy JSON | 2353 |
| Ulteriori informazioni | 2359 |

| | |
|-------------------------------------|------|
| AWSPriceListServiceFullAccess | 2360 |
| Utilizzo di questa politica | 2360 |
| Dettagli della politica | 2360 |
| Versione della politica | 2360 |
| Documento di policy JSON | 2360 |
| Ulteriori informazioni | 2361 |
| AWSPprivateCAAuditor | 2361 |
| Utilizzo di questa politica | 2361 |
| Dettagli della politica | 2361 |
| Versione della politica | 2361 |
| Documento di policy JSON | 2362 |
| Ulteriori informazioni | 2362 |
| AWSPprivateCAFullAccess | 2362 |
| Utilizzo di questa politica | 2363 |
| Dettagli della politica | 2363 |
| Versione della politica | 2363 |
| Documento di policy JSON | 2363 |
| Ulteriori informazioni | 2363 |
| AWSPprivateCAPrivilegedUser | 2364 |
| Utilizzo di questa politica | 2364 |
| Dettagli della politica | 2364 |
| Versione della politica | 2364 |
| Documento di policy JSON | 2364 |
| Ulteriori informazioni | 2366 |
| AWSPprivateCARedOnly | 2366 |
| Utilizzo di questa politica | 2366 |
| Dettagli della politica | 2366 |
| Versione della politica | 2366 |
| Documento di policy JSON | 2366 |
| Ulteriori informazioni | 2367 |
| AWSPprivateCAUser | 2367 |
| Utilizzo di questa politica | 2367 |
| Dettagli della politica | 2367 |
| Versione della politica | 2368 |
| Documento di policy JSON | 2368 |
| Ulteriori informazioni | 2369 |

| | |
|---|------|
| AWSPRivateMarketplaceAdminFullAccess | 2369 |
| Utilizzo di questa politica | 2369 |
| Dettagli della politica | 2370 |
| Versione della politica | 2370 |
| Documento di policy JSON | 2370 |
| Ulteriori informazioni | 2371 |
| AWSPRivateMarketplaceRequests | 2372 |
| Utilizzo di questa politica | 2372 |
| Dettagli della politica | 2372 |
| Versione della politica | 2372 |
| Documento di policy JSON | 2372 |
| Ulteriori informazioni | 2373 |
| AWSPRivateNetworksServiceRolePolicy | 2373 |
| Utilizzo di questa politica | 2373 |
| Dettagli della politica | 2373 |
| Versione della politica | 2373 |
| Documento di policy JSON | 2374 |
| Ulteriori informazioni | 2374 |
| AWSProtonCodeBuildProvisioningBasicAccess | 2374 |
| Utilizzo di questa politica | 2374 |
| Dettagli della politica | 2374 |
| Versione della politica | 2375 |
| Documento di policy JSON | 2375 |
| Ulteriori informazioni | 2375 |
| AWSProtonCodeBuildProvisioningServiceRolePolicy | 2376 |
| Utilizzo di questa politica | 2376 |
| Dettagli della politica | 2376 |
| Versione della politica | 2376 |
| Documento di policy JSON | 2376 |
| Ulteriori informazioni | 2378 |
| AWSProtonDeveloperAccess | 2378 |
| Utilizzo di questa politica | 2378 |
| Dettagli della politica | 2378 |
| Versione della politica | 2378 |
| Documento di policy JSON | 2378 |
| Ulteriori informazioni | 2381 |

| | |
|--|------|
| AWSProtonFullAccess | 2381 |
| Utilizzo di questa politica | 2381 |
| Dettagli della politica | 2381 |
| Versione della politica | 2381 |
| Documento di policy JSON | 2382 |
| Ulteriori informazioni | 2384 |
| AWSProtonReadOnlyAccess | 2384 |
| Utilizzo di questa politica | 2384 |
| Dettagli della politica | 2384 |
| Versione della politica | 2384 |
| Documento di policy JSON | 2385 |
| Ulteriori informazioni | 2386 |
| AWSProtonServiceGitSyncServiceRolePolicy | 2386 |
| Utilizzo di questa politica | 2386 |
| Dettagli della politica | 2386 |
| Versione della politica | 2387 |
| Documento di policy JSON | 2387 |
| Ulteriori informazioni | 2388 |
| AWSProtonSyncServiceRolePolicy | 2388 |
| Utilizzo di questa politica | 2388 |
| Dettagli della politica | 2388 |
| Versione della politica | 2388 |
| Documento di policy JSON | 2388 |
| Ulteriori informazioni | 2389 |
| AWSPurchaseOrdersServiceRolePolicy | 2390 |
| Utilizzo di questa politica | 2390 |
| Dettagli della politica | 2390 |
| Versione della politica | 2390 |
| Documento di policy JSON | 2390 |
| Ulteriori informazioni | 2391 |
| AWSQuickSightAssetBundleExportPolicy | 2391 |
| Utilizzo di questa politica | 2391 |
| Dettagli della politica | 2392 |
| Versione della politica | 2392 |
| Documento di policy JSON | 2392 |
| Ulteriori informazioni | 2394 |

| | |
|--|------|
| AWSQuickSightAssetBundleImportPolicy | 2394 |
| Utilizzo di questa politica | 2394 |
| Dettagli della politica | 2395 |
| Versione della politica | 2395 |
| Documento di policy JSON | 2395 |
| Ulteriori informazioni | 2398 |
| AWSQuickSightAthenaAccess | 2398 |
| Utilizzo di questa politica | 2398 |
| Dettagli della politica | 2398 |
| Versione della politica | 2399 |
| Documento di policy JSON | 2399 |
| Ulteriori informazioni | 2401 |
| AWSQuickSightDescribeRDS | 2401 |
| Utilizzo di questa politica | 2401 |
| Dettagli della politica | 2401 |
| Versione della politica | 2402 |
| Documento di policy JSON | 2402 |
| Ulteriori informazioni | 2402 |
| AWSQuickSightDescribeRedshift | 2402 |
| Utilizzo di questa politica | 2403 |
| Dettagli della politica | 2403 |
| Versione della politica | 2403 |
| Documento di policy JSON | 2403 |
| Ulteriori informazioni | 2403 |
| AWSQuickSightElasticsearchPolicy | 2404 |
| Utilizzo di questa politica | 2404 |
| Dettagli della politica | 2404 |
| Versione della politica | 2404 |
| Documento di policy JSON | 2404 |
| Ulteriori informazioni | 2405 |
| AWSQuickSightIoTAnalyticsAccess | 2406 |
| Utilizzo di questa politica | 2406 |
| Dettagli della politica | 2406 |
| Versione della politica | 2406 |
| Documento di policy JSON | 2406 |
| Ulteriori informazioni | 2407 |

| | |
|--|------|
| AWSQuickSightListIAM | 2407 |
| Utilizzo di questa politica | 2407 |
| Dettagli della politica | 2407 |
| Versione della politica | 2407 |
| Documento di policy JSON | 2408 |
| Ulteriori informazioni | 2408 |
| AWSQuickSightOpenSearchPolicy | 2408 |
| Utilizzo di questa politica | 2408 |
| Dettagli della politica | 2408 |
| Versione della politica | 2409 |
| Documento di policy JSON | 2409 |
| Ulteriori informazioni | 2410 |
| AWSQuickSightSageMakerPolicy | 2410 |
| Utilizzo di questa politica | 2410 |
| Dettagli della politica | 2410 |
| Versione della politica | 2410 |
| Documento di policy JSON | 2411 |
| Ulteriori informazioni | 2412 |
| AWSQuickSightTimestreamPolicy | 2412 |
| Utilizzo di questa politica | 2412 |
| Dettagli della politica | 2412 |
| Versione della politica | 2413 |
| Documento di policy JSON | 2413 |
| Ulteriori informazioni | 2413 |
| AWSReachabilityAnalyzerServiceRolePolicy | 2414 |
| Utilizzo di questa politica | 2414 |
| Dettagli della politica | 2414 |
| Versione della politica | 2414 |
| Documento di policy JSON | 2414 |
| Ulteriori informazioni | 2417 |
| AWSRefactoringToolkitFullAccess | 2417 |
| Utilizzo di questa politica | 2417 |
| Dettagli della politica | 2417 |
| Versione della politica | 2417 |
| Documento di policy JSON | 2418 |
| Ulteriori informazioni | 2431 |

| | |
|---|------|
| AWSRefactoringToolkitSidecarPolicy | 2431 |
| Utilizzo di questa politica | 2431 |
| Dettagli della politica | 2432 |
| Versione della politica | 2432 |
| Documento di policy JSON | 2432 |
| Ulteriori informazioni | 2433 |
| AWSRePostPrivateCloudWatchAccess | 2433 |
| Utilizzo di questa politica | 2433 |
| Dettagli della politica | 2433 |
| Versione della politica | 2434 |
| Documento di policy JSON | 2434 |
| Ulteriori informazioni | 2434 |
| AWSRepostSpaceSupportOperationsPolicy | 2435 |
| Utilizzo di questa politica | 2435 |
| Dettagli della politica | 2435 |
| Versione della politica | 2435 |
| Documento di policy JSON | 2435 |
| Ulteriori informazioni | 2436 |
| AWSResilienceHubAssessmentExecutionPolicy | 2436 |
| Utilizzo di questa politica | 2436 |
| Dettagli della politica | 2436 |
| Versione della politica | 2436 |
| Documento di policy JSON | 2437 |
| Ulteriori informazioni | 2441 |
| AWSResourceAccessManagerFullAccess | 2441 |
| Utilizzo di questa politica | 2441 |
| Dettagli della politica | 2441 |
| Versione della politica | 2441 |
| Documento di policy JSON | 2442 |
| Ulteriori informazioni | 2442 |
| AWSResourceAccessManagerReadOnlyAccess | 2442 |
| Utilizzo di questa politica | 2442 |
| Dettagli della politica | 2442 |
| Versione della politica | 2443 |
| Documento di policy JSON | 2443 |
| Ulteriori informazioni | 2443 |

| | |
|--|------|
| AWSResourceAccessManagerResourceShareParticipantAccess | 2443 |
| Utilizzo di questa politica | 2444 |
| Dettagli della politica | 2444 |
| Versione della politica | 2444 |
| Documento di policy JSON | 2444 |
| Ulteriori informazioni | 2445 |
| AWSResourceAccessManagerServiceRolePolicy | 2445 |
| Utilizzo di questa politica | 2445 |
| Dettagli della politica | 2445 |
| Versione della politica | 2445 |
| Documento di policy JSON | 2446 |
| Ulteriori informazioni | 2446 |
| AWSResourceExplorerFullAccess | 2447 |
| Utilizzo di questa politica | 2447 |
| Dettagli della politica | 2447 |
| Versione della politica | 2447 |
| Documento di policy JSON | 2447 |
| Ulteriori informazioni | 2448 |
| AWSResourceExplorerOrganizationsAccess | 2448 |
| Utilizzo di questa politica | 2449 |
| Dettagli della politica | 2449 |
| Versione della politica | 2449 |
| Documento di policy JSON | 2449 |
| Ulteriori informazioni | 2451 |
| AWSResourceExplorerReadOnlyAccess | 2451 |
| Utilizzo di questa politica | 2451 |
| Dettagli della politica | 2451 |
| Versione della politica | 2451 |
| Documento di policy JSON | 2452 |
| Ulteriori informazioni | 2452 |
| AWSResourceExplorerServiceRolePolicy | 2452 |
| Utilizzo di questa politica | 2453 |
| Dettagli della politica | 2453 |
| Versione della politica | 2453 |
| Documento di policy JSON | 2453 |
| Ulteriori informazioni | 2462 |

| | |
|---------------------------------------|------|
| AWSResourceGroupsReadOnlyAccess | 2462 |
| Utilizzo di questa politica | 2462 |
| Dettagli della politica | 2463 |
| Versione della politica | 2463 |
| Documento di policy JSON | 2463 |
| Ulteriori informazioni | 2464 |
| AWSRoboMaker_FullAccess | 2465 |
| Utilizzo di questa politica | 2465 |
| Dettagli della politica | 2465 |
| Versione della politica | 2465 |
| Documento di policy JSON | 2465 |
| Ulteriori informazioni | 2466 |
| AWSRoboMakerReadOnlyAccess | 2467 |
| Utilizzo di questa politica | 2467 |
| Dettagli della politica | 2467 |
| Versione della politica | 2467 |
| Documento di policy JSON | 2467 |
| Ulteriori informazioni | 2468 |
| AWSRoboMakerServicePolicy | 2468 |
| Utilizzo di questa politica | 2468 |
| Dettagli della politica | 2468 |
| Versione della politica | 2468 |
| Documento di policy JSON | 2469 |
| Ulteriori informazioni | 2470 |
| AWSRoboMakerServiceRolePolicy | 2470 |
| Utilizzo di questa politica | 2471 |
| Dettagli della politica | 2471 |
| Versione della politica | 2471 |
| Documento di policy JSON | 2471 |
| Ulteriori informazioni | 2472 |
| AWSRolesAnywhereServicePolicy | 2472 |
| Utilizzo di questa politica | 2473 |
| Dettagli della politica | 2473 |
| Versione della politica | 2473 |
| Documento di policy JSON | 2473 |
| Ulteriori informazioni | 2474 |

| | |
|---|------|
| AWSS3OnOutpostsServiceRolePolicy | 2474 |
| Utilizzo di questa politica | 2474 |
| Dettagli della politica | 2474 |
| Versione della politica | 2475 |
| Documento di policy JSON | 2475 |
| Ulteriori informazioni | 2477 |
| AWSSavingsPlansFullAccess | 2477 |
| Utilizzo di questa politica | 2478 |
| Dettagli della politica | 2478 |
| Versione della politica | 2478 |
| Documento di policy JSON | 2478 |
| Ulteriori informazioni | 2478 |
| AWSSavingsPlansReadOnlyAccess | 2479 |
| Utilizzo di questa politica | 2479 |
| Dettagli della politica | 2479 |
| Versione della politica | 2479 |
| Documento di policy JSON | 2479 |
| Ulteriori informazioni | 2480 |
| AWSSecurityHubFullAccess | 2480 |
| Utilizzo di questa politica | 2480 |
| Dettagli della politica | 2480 |
| Versione della politica | 2480 |
| Documento di policy JSON | 2481 |
| Ulteriori informazioni | 2481 |
| AWSSecurityHubOrganizationsAccess | 2482 |
| Utilizzo di questa politica | 2482 |
| Dettagli della politica | 2482 |
| Versione della politica | 2482 |
| Documento di policy JSON | 2482 |
| Ulteriori informazioni | 2483 |
| AWSSecurityHubReadOnlyAccess | 2484 |
| Utilizzo di questa politica | 2484 |
| Dettagli della politica | 2484 |
| Versione della politica | 2484 |
| Documento di policy JSON | 2484 |
| Ulteriori informazioni | 2485 |

| | |
|---|------|
| AWSSecurityHubServiceRolePolicy | 2485 |
| Utilizzo di questa politica | 2485 |
| Dettagli della politica | 2485 |
| Versione della politica | 2485 |
| Documento di policy JSON | 2486 |
| Ulteriori informazioni | 2488 |
| AWSServiceCatalogAdminFullAccess | 2488 |
| Utilizzo di questa politica | 2488 |
| Dettagli della politica | 2488 |
| Versione della politica | 2488 |
| Documento di policy JSON | 2488 |
| Ulteriori informazioni | 2491 |
| AWSServiceCatalogAdminReadOnlyAccess | 2491 |
| Utilizzo di questa politica | 2491 |
| Dettagli della politica | 2492 |
| Versione della politica | 2492 |
| Documento di policy JSON | 2492 |
| Ulteriori informazioni | 2493 |
| AWSServiceCatalogAppRegistryFullAccess | 2493 |
| Utilizzo di questa politica | 2494 |
| Dettagli della politica | 2494 |
| Versione della politica | 2494 |
| Documento di policy JSON | 2494 |
| Ulteriori informazioni | 2496 |
| AWSServiceCatalogAppRegistryReadOnlyAccess | 2496 |
| Utilizzo di questa politica | 2497 |
| Dettagli della politica | 2497 |
| Versione della politica | 2497 |
| Documento di policy JSON | 2497 |
| Ulteriori informazioni | 2498 |
| AWSServiceCatalogAppRegistryServiceRolePolicy | 2498 |
| Utilizzo di questa politica | 2498 |
| Dettagli della politica | 2498 |
| Versione della politica | 2498 |
| Documento di policy JSON | 2499 |
| Ulteriori informazioni | 2500 |

| | |
|--|------|
| AWSServiceCatalogEndUserFullAccess | 2500 |
| Utilizzo di questa politica | 2500 |
| Dettagli della politica | 2500 |
| Versione della politica | 2500 |
| Documento di policy JSON | 2501 |
| Ulteriori informazioni | 2503 |
| AWSServiceCatalogEndUserReadOnlyAccess | 2503 |
| Utilizzo di questa politica | 2503 |
| Dettagli della politica | 2503 |
| Versione della politica | 2503 |
| Documento di policy JSON | 2503 |
| Ulteriori informazioni | 2505 |
| AWSServiceCatalogOrgsDataSyncServiceRolePolicy | 2505 |
| Utilizzo di questa politica | 2505 |
| Dettagli della politica | 2506 |
| Versione della politica | 2506 |
| Documento di policy JSON | 2506 |
| Ulteriori informazioni | 2507 |
| AWSServiceCatalogSyncServiceRolePolicy | 2507 |
| Utilizzo di questa politica | 2507 |
| Dettagli della politica | 2507 |
| Versione della politica | 2507 |
| Documento di policy JSON | 2507 |
| Ulteriori informazioni | 2508 |
| AWSServiceRoleForAmazonEKSNodegroup | 2509 |
| Utilizzo di questa politica | 2509 |
| Dettagli della politica | 2509 |
| Versione della politica | 2509 |
| Documento di policy JSON | 2509 |
| Ulteriori informazioni | 2513 |
| AWSServiceRoleForAmazonQDeveloper | 2514 |
| Utilizzo di questa politica | 2514 |
| Dettagli della politica | 2514 |
| Versione della politica | 2514 |
| Documento di policy JSON | 2514 |
| Ulteriori informazioni | 2515 |

| | |
|--|------|
| AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy | 2515 |
| Utilizzo di questa politica | 2515 |
| Dettagli della politica | 2515 |
| Versione della politica | 2516 |
| Documento di policy JSON | 2516 |
| Ulteriori informazioni | 2516 |
| AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy | 2516 |
| Utilizzo di questa politica | 2516 |
| Dettagli della politica | 2517 |
| Versione della politica | 2517 |
| Documento di policy JSON | 2517 |
| Ulteriori informazioni | 2517 |
| AWSServiceRoleForCodeGuru-Profiler | 2518 |
| Utilizzo di questa politica | 2518 |
| Dettagli della politica | 2518 |
| Versione della politica | 2518 |
| Documento di policy JSON | 2518 |
| Ulteriori informazioni | 2519 |
| AWSServiceRoleForCodeWhispererPolicy | 2519 |
| Utilizzo di questa politica | 2519 |
| Dettagli della politica | 2519 |
| Versione della politica | 2519 |
| Documento di policy JSON | 2520 |
| Ulteriori informazioni | 2521 |
| AWSServiceRoleForEC2ScheduledInstances | 2522 |
| Utilizzo di questa politica | 2522 |
| Dettagli della politica | 2522 |
| Versione della politica | 2522 |
| Documento di policy JSON | 2522 |
| Ulteriori informazioni | 2523 |
| AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy | 2523 |
| Utilizzo di questa politica | 2523 |
| Dettagli della politica | 2524 |
| Versione della politica | 2524 |
| Documento di policy JSON | 2524 |
| Ulteriori informazioni | 2524 |

| | |
|--|------|
| AWSServiceRoleForImageBuilder | 2525 |
| Utilizzo di questa politica | 2525 |
| Dettagli della politica | 2525 |
| Versione della politica | 2525 |
| Documento di policy JSON | 2525 |
| Ulteriori informazioni | 2535 |
| AWSServiceRoleForIoTSiteWise | 2535 |
| Utilizzo di questa politica | 2535 |
| Dettagli della politica | 2535 |
| Versione della politica | 2536 |
| Documento di policy JSON | 2536 |
| Ulteriori informazioni | 2537 |
| AWSServiceRoleForLogDeliveryPolicy | 2537 |
| Utilizzo di questa politica | 2537 |
| Dettagli della politica | 2537 |
| Versione della politica | 2538 |
| Documento di policy JSON | 2538 |
| Ulteriori informazioni | 2538 |
| AWSServiceRoleForMonitronPolicy | 2539 |
| Utilizzo di questa politica | 2539 |
| Dettagli della politica | 2539 |
| Versione della politica | 2539 |
| Documento di policy JSON | 2539 |
| Ulteriori informazioni | 2540 |
| AWSServiceRoleForNeptuneGraphPolicy | 2540 |
| Utilizzo di questa politica | 2540 |
| Dettagli della politica | 2540 |
| Versione della politica | 2540 |
| Documento di policy JSON | 2541 |
| Ulteriori informazioni | 2542 |
| AWSServiceRoleForPrivateMarketplaceAdminPolicy | 2542 |
| Utilizzo di questa politica | 2542 |
| Dettagli della politica | 2542 |
| Versione della politica | 2543 |
| Documento di policy JSON | 2543 |
| Ulteriori informazioni | 2544 |

| | |
|---|------|
| AWSServiceRoleForSMS | 2545 |
| Utilizzo di questa politica | 2545 |
| Dettagli della politica | 2545 |
| Versione della politica | 2545 |
| Documento di policy JSON | 2545 |
| Ulteriori informazioni | 2552 |
| AWSServiceRoleForUserSubscriptions | 2552 |
| Utilizzo di questa politica | 2552 |
| Dettagli della politica | 2552 |
| Versione della politica | 2553 |
| Documento di policy JSON | 2553 |
| Ulteriori informazioni | 2553 |
| AWSServiceRolePolicyForBackupReports | 2554 |
| Utilizzo di questa politica | 2554 |
| Dettagli della politica | 2554 |
| Versione della politica | 2554 |
| Documento di policy JSON | 2554 |
| Ulteriori informazioni | 2555 |
| AWSServiceRolePolicyForBackupRestoreTesting | 2556 |
| Utilizzo di questa politica | 2556 |
| Dettagli della politica | 2556 |
| Versione della politica | 2556 |
| Documento di policy JSON | 2556 |
| Ulteriori informazioni | 2559 |
| AWSShieldDRTAccessPolicy | 2559 |
| Utilizzo di questa politica | 2559 |
| Dettagli della politica | 2559 |
| Versione della politica | 2560 |
| Documento di policy JSON | 2560 |
| Ulteriori informazioni | 2561 |
| AWSShieldServiceRolePolicy | 2561 |
| Utilizzo di questa politica | 2561 |
| Dettagli della politica | 2561 |
| Versione della politica | 2561 |
| Documento di policy JSON | 2562 |
| Ulteriori informazioni | 2562 |

| | |
|---|------|
| AWSSSMForSAPServiceLinkedRolePolicy | 2562 |
| Utilizzo di questa politica | 2563 |
| Dettagli della politica | 2563 |
| Versione della politica | 2563 |
| Documento di policy JSON | 2563 |
| Ulteriori informazioni | 2570 |
| AWSSSMOpsInsightsServiceRolePolicy | 2570 |
| Utilizzo di questa politica | 2570 |
| Dettagli della politica | 2570 |
| Versione della politica | 2570 |
| Documento di policy JSON | 2570 |
| Ulteriori informazioni | 2571 |
| AWSSSODirectoryAdministrator | 2571 |
| Utilizzo di questa politica | 2571 |
| Dettagli della politica | 2572 |
| Versione della politica | 2572 |
| Documento di policy JSON | 2572 |
| Ulteriori informazioni | 2572 |
| AWSSSODirectoryReadOnly | 2573 |
| Utilizzo di questa politica | 2573 |
| Dettagli della politica | 2573 |
| Versione della politica | 2573 |
| Documento di policy JSON | 2573 |
| Ulteriori informazioni | 2574 |
| AWSSSOMasterAccountAdministrator | 2574 |
| Utilizzo di questa politica | 2574 |
| Dettagli della politica | 2574 |
| Versione della politica | 2575 |
| Documento di policy JSON | 2575 |
| Ulteriori informazioni | 2577 |
| AWSSSOMemberAccountAdministrator | 2577 |
| Utilizzo di questa politica | 2577 |
| Dettagli della politica | 2577 |
| Versione della politica | 2577 |
| Documento di policy JSON | 2577 |
| Ulteriori informazioni | 2579 |

| | |
|--|------|
| AWSSSOReadOnly | 2579 |
| Utilizzo di questa politica | 2579 |
| Dettagli della politica | 2579 |
| Versione della politica | 2579 |
| Documento di policy JSON | 2580 |
| Ulteriori informazioni | 2580 |
| AWSSSOServiceRolePolicy | 2581 |
| Utilizzo di questa politica | 2581 |
| Dettagli della politica | 2581 |
| Versione della politica | 2581 |
| Documento di policy JSON | 2581 |
| Ulteriori informazioni | 2585 |
| AWSSStepFunctionsConsoleFullAccess | 2585 |
| Utilizzo di questa politica | 2585 |
| Dettagli della politica | 2585 |
| Versione della politica | 2585 |
| Documento di policy JSON | 2586 |
| Ulteriori informazioni | 2586 |
| AWSSStepFunctionsFullAccess | 2587 |
| Utilizzo di questa politica | 2587 |
| Dettagli della politica | 2587 |
| Versione della politica | 2587 |
| Documento di policy JSON | 2587 |
| Ulteriori informazioni | 2588 |
| AWSSStepFunctionsReadOnlyAccess | 2588 |
| Utilizzo di questa politica | 2588 |
| Dettagli della politica | 2588 |
| Versione della politica | 2588 |
| Documento di policy JSON | 2588 |
| Ulteriori informazioni | 2589 |
| AWSSStorageGatewayFullAccess | 2589 |
| Utilizzo di questa politica | 2590 |
| Dettagli della politica | 2590 |
| Versione della politica | 2590 |
| Documento di policy JSON | 2590 |
| Ulteriori informazioni | 2591 |

| | |
|---|------|
| AWSSStorageGatewayReadOnlyAccess | 2591 |
| Utilizzo di questa politica | 2591 |
| Dettagli della politica | 2591 |
| Versione della politica | 2591 |
| Documento di policy JSON | 2592 |
| Ulteriori informazioni | 2592 |
| AWSSStorageGatewayServiceRolePolicy | 2593 |
| Utilizzo di questa politica | 2593 |
| Dettagli della politica | 2593 |
| Versione della politica | 2593 |
| Documento di policy JSON | 2593 |
| Ulteriori informazioni | 2594 |
| AWSSupplyChainFederationAdminAccess | 2594 |
| Utilizzo di questa politica | 2594 |
| Dettagli della politica | 2594 |
| Versione della politica | 2594 |
| Documento di policy JSON | 2595 |
| Ulteriori informazioni | 2600 |
| AWSSupportAccess | 2600 |
| Utilizzo di questa politica | 2600 |
| Dettagli della politica | 2600 |
| Versione della politica | 2601 |
| Documento di policy JSON | 2601 |
| Ulteriori informazioni | 2601 |
| AWSSupportAppFullAccess | 2601 |
| Utilizzo di questa politica | 2602 |
| Dettagli della politica | 2602 |
| Versione della politica | 2602 |
| Documento di policy JSON | 2602 |
| Ulteriori informazioni | 2603 |
| AWSSupportAppReadOnlyAccess | 2603 |
| Utilizzo di questa politica | 2603 |
| Dettagli della politica | 2603 |
| Versione della politica | 2604 |
| Documento di policy JSON | 2604 |
| Ulteriori informazioni | 2604 |

| | |
|--|------|
| AWSSupportPlansFullAccess | 2604 |
| Utilizzo di questa politica | 2604 |
| Dettagli della politica | 2605 |
| Versione della politica | 2605 |
| Documento di policy JSON | 2605 |
| Ulteriori informazioni | 2605 |
| AWSSupportPlansReadOnlyAccess | 2606 |
| Utilizzo di questa politica | 2606 |
| Dettagli della politica | 2606 |
| Versione della politica | 2606 |
| Documento di policy JSON | 2606 |
| Ulteriori informazioni | 2607 |
| AWSSupportServiceRolePolicy | 2607 |
| Utilizzo di questa politica | 2607 |
| Dettagli della politica | 2607 |
| Versione della politica | 2607 |
| Documento di policy JSON | 2608 |
| Ulteriori informazioni | 2683 |
| AWSSystemsManagerAccountDiscoveryServicePolicy | 2683 |
| Utilizzo di questa politica | 2683 |
| Dettagli della politica | 2683 |
| Versione della politica | 2684 |
| Documento di policy JSON | 2684 |
| Ulteriori informazioni | 2684 |
| AWSSystemsManagerChangeManagementServicePolicy | 2685 |
| Utilizzo di questa politica | 2685 |
| Dettagli della politica | 2685 |
| Versione della politica | 2685 |
| Documento di policy JSON | 2685 |
| Ulteriori informazioni | 2687 |
| AWSSystemsManagerForSAPFullAccess | 2687 |
| Utilizzo di questa politica | 2687 |
| Dettagli della politica | 2687 |
| Versione della politica | 2688 |
| Documento di policy JSON | 2688 |
| Ulteriori informazioni | 2688 |

| | |
|---|------|
| AWSSystemsManagerForSAPReadOnlyAccess | 2689 |
| Utilizzo di questa politica | 2689 |
| Dettagli della politica | 2689 |
| Versione della politica | 2689 |
| Documento di policy JSON | 2689 |
| Ulteriori informazioni | 2690 |
| AWSSystemsManagerOpsDataSyncServiceRolePolicy | 2690 |
| Utilizzo di questa politica | 2690 |
| Dettagli della politica | 2690 |
| Versione della politica | 2690 |
| Documento di policy JSON | 2691 |
| Ulteriori informazioni | 2694 |
| AWSThinkboxAssetServerPolicy | 2694 |
| Utilizzo di questa politica | 2695 |
| Dettagli della politica | 2695 |
| Versione della politica | 2695 |
| Documento di policy JSON | 2695 |
| Ulteriori informazioni | 2696 |
| AWSThinkboxAWSPortalAdminPolicy | 2696 |
| Utilizzo di questa politica | 2696 |
| Dettagli della politica | 2696 |
| Versione della politica | 2696 |
| Documento di policy JSON | 2697 |
| Ulteriori informazioni | 2706 |
| AWSThinkboxAWSPortalGatewayPolicy | 2707 |
| Utilizzo di questa politica | 2707 |
| Dettagli della politica | 2707 |
| Versione della politica | 2707 |
| Documento di policy JSON | 2707 |
| Ulteriori informazioni | 2709 |
| AWSThinkboxAWSPortalWorkerPolicy | 2709 |
| Utilizzo di questa politica | 2709 |
| Dettagli della politica | 2710 |
| Versione della politica | 2710 |
| Documento di policy JSON | 2710 |
| Ulteriori informazioni | 2712 |

| | |
|--|------|
| AWSThinkboxDeadlineResourceTrackerAccessPolicy | 2712 |
| Utilizzo di questa politica | 2712 |
| Dettagli della politica | 2712 |
| Versione della politica | 2713 |
| Documento di policy JSON | 2713 |
| Ulteriori informazioni | 2716 |
| AWSThinkboxDeadlineResourceTrackerAdminPolicy | 2716 |
| Utilizzo di questa politica | 2716 |
| Dettagli della politica | 2716 |
| Versione della politica | 2716 |
| Documento di policy JSON | 2717 |
| Ulteriori informazioni | 2722 |
| AWSThinkboxDeadlineSpotEventPluginAdminPolicy | 2723 |
| Utilizzo di questa politica | 2723 |
| Dettagli della politica | 2723 |
| Versione della politica | 2723 |
| Documento di policy JSON | 2723 |
| Ulteriori informazioni | 2726 |
| AWSThinkboxDeadlineSpotEventPluginWorkerPolicy | 2726 |
| Utilizzo di questa politica | 2726 |
| Dettagli della politica | 2727 |
| Versione della politica | 2727 |
| Documento di policy JSON | 2727 |
| Ulteriori informazioni | 2728 |
| AWSTransferConsoleFullAccess | 2729 |
| Utilizzo di questa politica | 2729 |
| Dettagli della politica | 2729 |
| Versione della politica | 2729 |
| Documento di policy JSON | 2729 |
| Ulteriori informazioni | 2730 |
| AWSTransferFullAccess | 2730 |
| Utilizzo di questa politica | 2730 |
| Dettagli della politica | 2731 |
| Versione della politica | 2731 |
| Documento di policy JSON | 2731 |
| Ulteriori informazioni | 2732 |

| | |
|---|------|
| AWSTransferLoggingAccess | 2732 |
| Utilizzo di questa politica | 2732 |
| Dettagli della politica | 2732 |
| Versione della politica | 2732 |
| Documento di policy JSON | 2733 |
| Ulteriori informazioni | 2733 |
| AWSTransferReadOnlyAccess | 2733 |
| Utilizzo di questa politica | 2733 |
| Dettagli della politica | 2734 |
| Versione della politica | 2734 |
| Documento di policy JSON | 2734 |
| Ulteriori informazioni | 2734 |
| AWSTrustedAdvisorPriorityFullAccess | 2735 |
| Utilizzo di questa politica | 2735 |
| Dettagli della politica | 2735 |
| Versione della politica | 2735 |
| Documento di policy JSON | 2735 |
| Ulteriori informazioni | 2737 |
| AWSTrustedAdvisorPriorityReadOnlyAccess | 2737 |
| Utilizzo di questa politica | 2737 |
| Dettagli della politica | 2738 |
| Versione della politica | 2738 |
| Documento di policy JSON | 2738 |
| Ulteriori informazioni | 2739 |
| AWSTrustedAdvisorReportingServiceRolePolicy | 2739 |
| Utilizzo di questa politica | 2739 |
| Dettagli della politica | 2739 |
| Versione della politica | 2740 |
| Documento di policy JSON | 2740 |
| Ulteriori informazioni | 2740 |
| AWSTrustedAdvisorServiceRolePolicy | 2741 |
| Utilizzo di questa politica | 2741 |
| Dettagli della politica | 2741 |
| Versione della politica | 2741 |
| Documento di policy JSON | 2741 |
| Ulteriori informazioni | 2744 |

| | |
|---|------|
| AWSUserNotificationsServiceLinkedRolePolicy | 2744 |
| Utilizzo di questa politica | 2744 |
| Dettagli della politica | 2745 |
| Versione della politica | 2745 |
| Documento di policy JSON | 2745 |
| Ulteriori informazioni | 2746 |
| AWSVendorInsightsAssessorFullAccess | 2746 |
| Utilizzo di questa politica | 2746 |
| Dettagli della politica | 2746 |
| Versione della politica | 2746 |
| Documento di policy JSON | 2747 |
| Ulteriori informazioni | 2748 |
| AWSVendorInsightsAssessorReadOnly | 2748 |
| Utilizzo di questa politica | 2748 |
| Dettagli della politica | 2748 |
| Versione della politica | 2748 |
| Documento di policy JSON | 2749 |
| Ulteriori informazioni | 2749 |
| AWSVendorInsightsVendorFullAccess | 2749 |
| Utilizzo di questa politica | 2750 |
| Dettagli della politica | 2750 |
| Versione della politica | 2750 |
| Documento di policy JSON | 2750 |
| Ulteriori informazioni | 2752 |
| AWSVendorInsightsVendorReadOnly | 2752 |
| Utilizzo di questa politica | 2752 |
| Dettagli della politica | 2752 |
| Versione della politica | 2752 |
| Documento di policy JSON | 2753 |
| Ulteriori informazioni | 2754 |
| AWSVpcLatticeServiceRolePolicy | 2754 |
| Utilizzo di questa politica | 2754 |
| Dettagli della politica | 2754 |
| Versione della politica | 2754 |
| Documento di policy JSON | 2754 |
| Ulteriori informazioni | 2755 |

| | |
|---|------|
| AWSVPCS2SVpnServiceRolePolicy | 2755 |
| Utilizzo di questa politica | 2755 |
| Dettagli della politica | 2755 |
| Versione della politica | 2756 |
| Documento di policy JSON | 2756 |
| Ulteriori informazioni | 2756 |
| AWSVPCTransitGatewayServiceRolePolicy | 2756 |
| Utilizzo di questa politica | 2757 |
| Dettagli della politica | 2757 |
| Versione della politica | 2757 |
| Documento di policy JSON | 2757 |
| Ulteriori informazioni | 2758 |
| AWSVPCVerifiedAccessServiceRolePolicy | 2758 |
| Utilizzo di questa politica | 2758 |
| Dettagli della politica | 2758 |
| Versione della politica | 2758 |
| Documento di policy JSON | 2759 |
| Ulteriori informazioni | 2760 |
| AWSWAFConsoleFullAccess | 2760 |
| Utilizzo di questa politica | 2761 |
| Dettagli della politica | 2761 |
| Versione della politica | 2761 |
| Documento di policy JSON | 2761 |
| Ulteriori informazioni | 2763 |
| AWSWAFConsoleReadOnlyAccess | 2763 |
| Utilizzo di questa politica | 2763 |
| Dettagli della politica | 2764 |
| Versione della politica | 2764 |
| Documento di policy JSON | 2764 |
| Ulteriori informazioni | 2765 |
| AWSWAFFullAccess | 2765 |
| Utilizzo di questa politica | 2765 |
| Dettagli della politica | 2765 |
| Versione della politica | 2766 |
| Documento di policy JSON | 2766 |
| Ulteriori informazioni | 2767 |

| | |
|--|------|
| AWSWAFAReadOnlyAccess | 2768 |
| Utilizzo di questa politica | 2768 |
| Dettagli della politica | 2768 |
| Versione della politica | 2768 |
| Documento di policy JSON | 2768 |
| Ulteriori informazioni | 2769 |
| AWSWellArchitectedDiscoveryServiceRolePolicy | 2769 |
| Utilizzo di questa politica | 2769 |
| Dettagli della politica | 2769 |
| Versione della politica | 2770 |
| Documento di policy JSON | 2770 |
| Ulteriori informazioni | 2771 |
| AWSWellArchitectedOrganizationsServiceRolePolicy | 2771 |
| Utilizzo di questa politica | 2772 |
| Dettagli della politica | 2772 |
| Versione della politica | 2772 |
| Documento di policy JSON | 2772 |
| Ulteriori informazioni | 2773 |
| AWSWickrFullAccess | 2773 |
| Utilizzo di questa politica | 2773 |
| Dettagli della politica | 2773 |
| Versione della politica | 2773 |
| Documento di policy JSON | 2773 |
| Ulteriori informazioni | 2774 |
| AWSXrayCrossAccountSharingConfiguration | 2774 |
| Utilizzo di questa politica | 2774 |
| Dettagli della politica | 2774 |
| Versione della politica | 2774 |
| Documento di policy JSON | 2775 |
| Ulteriori informazioni | 2776 |
| AWSXRayDaemonWriteAccess | 2776 |
| Utilizzo di questa politica | 2776 |
| Dettagli della politica | 2776 |
| Versione della politica | 2776 |
| Documento di policy JSON | 2776 |
| Ulteriori informazioni | 2777 |

| | |
|---|------|
| AWSXrayFullAccess | 2777 |
| Utilizzo di questa politica | 2777 |
| Dettagli della politica | 2777 |
| Versione della politica | 2778 |
| Documento di policy JSON | 2778 |
| Ulteriori informazioni | 2778 |
| AWSXrayReadOnlyAccess | 2779 |
| Utilizzo di questa politica | 2779 |
| Dettagli della politica | 2779 |
| Versione della politica | 2779 |
| Documento di policy JSON | 2779 |
| Ulteriori informazioni | 2780 |
| AWSXrayWriteOnlyAccess | 2780 |
| Utilizzo di questa politica | 2780 |
| Dettagli della politica | 2780 |
| Versione della politica | 2781 |
| Documento di policy JSON | 2781 |
| Ulteriori informazioni | 2781 |
| AWSZonalAutoshiftPracticeRunSLRPolicy | 2782 |
| Utilizzo di questa politica | 2782 |
| Dettagli della politica | 2782 |
| Versione della politica | 2782 |
| Documento di policy JSON | 2782 |
| Ulteriori informazioni | 2783 |
| BatchServiceRolePolicy | 2783 |
| Utilizzo di questa politica | 2783 |
| Dettagli della politica | 2783 |
| Versione della politica | 2784 |
| Documento di policy JSON | 2784 |
| Ulteriori informazioni | 2790 |
| Billing | 2790 |
| Utilizzo di questa politica | 2790 |
| Dettagli della politica | 2790 |
| Versione della politica | 2790 |
| Documento di policy JSON | 2791 |
| Ulteriori informazioni | 2793 |

| | |
|---|------|
| CertificateManagerServiceRolePolicy | 2794 |
| Utilizzo di questa politica | 2794 |
| Dettagli della politica | 2794 |
| Versione della politica | 2794 |
| Documento di policy JSON | 2794 |
| Ulteriori informazioni | 2795 |
| ClientVPNServiceConnectionsRolePolicy | 2795 |
| Utilizzo di questa politica | 2795 |
| Dettagli della politica | 2795 |
| Versione della politica | 2795 |
| Documento di policy JSON | 2796 |
| Ulteriori informazioni | 2796 |
| ClientVPNServiceRolePolicy | 2796 |
| Utilizzo di questa politica | 2796 |
| Dettagli della politica | 2796 |
| Versione della politica | 2797 |
| Documento di policy JSON | 2797 |
| Ulteriori informazioni | 2798 |
| CloudFormationStackSetsOrgAdminServiceRolePolicy | 2798 |
| Utilizzo di questa politica | 2798 |
| Dettagli della politica | 2798 |
| Versione della politica | 2798 |
| Documento di policy JSON | 2799 |
| Ulteriori informazioni | 2799 |
| CloudFormationStackSetsOrgMemberServiceRolePolicy | 2799 |
| Utilizzo di questa politica | 2799 |
| Dettagli della politica | 2800 |
| Versione della politica | 2800 |
| Documento di policy JSON | 2800 |
| Ulteriori informazioni | 2801 |
| CloudFrontFullAccess | 2801 |
| Utilizzo di questa politica | 2801 |
| Dettagli della politica | 2801 |
| Versione della politica | 2801 |
| Documento di policy JSON | 2802 |
| Ulteriori informazioni | 2803 |

| | |
|-------------------------------------|------|
| CloudFrontReadOnlyAccess | 2803 |
| Utilizzo di questa politica | 2803 |
| Dettagli della politica | 2803 |
| Versione della politica | 2803 |
| Documento di policy JSON | 2804 |
| Ulteriori informazioni | 2804 |
| CloudHSMServiceRolePolicy | 2805 |
| Utilizzo di questa politica | 2805 |
| Dettagli della politica | 2805 |
| Versione della politica | 2805 |
| Documento di policy JSON | 2805 |
| Ulteriori informazioni | 2806 |
| CloudSearchFullAccess | 2806 |
| Utilizzo di questa politica | 2806 |
| Dettagli della politica | 2806 |
| Versione della politica | 2806 |
| Documento di policy JSON | 2807 |
| Ulteriori informazioni | 2807 |
| CloudSearchReadOnlyAccess | 2807 |
| Utilizzo di questa politica | 2807 |
| Dettagli della politica | 2807 |
| Versione della politica | 2808 |
| Documento di policy JSON | 2808 |
| Ulteriori informazioni | 2808 |
| CloudTrailServiceRolePolicy | 2808 |
| Utilizzo di questa politica | 2809 |
| Dettagli della politica | 2809 |
| Versione della politica | 2809 |
| Documento di policy JSON | 2809 |
| Ulteriori informazioni | 2811 |
| CloudWatch-CrossAccountAccess | 2811 |
| Utilizzo di questa politica | 2811 |
| Dettagli della politica | 2811 |
| Versione della politica | 2811 |
| Documento di policy JSON | 2812 |
| Ulteriori informazioni | 2812 |

| | |
|--|------|
| CloudWatchActionsEC2Access | 2812 |
| Utilizzo di questa politica | 2812 |
| Dettagli della politica | 2812 |
| Versione della politica | 2813 |
| Documento di policy JSON | 2813 |
| Ulteriori informazioni | 2813 |
| CloudWatchAgentAdminPolicy | 2813 |
| Utilizzo di questa politica | 2814 |
| Dettagli della politica | 2814 |
| Versione della politica | 2814 |
| Documento di policy JSON | 2814 |
| Ulteriori informazioni | 2815 |
| CloudWatchAgentServerPolicy | 2815 |
| Utilizzo di questa politica | 2815 |
| Dettagli della politica | 2815 |
| Versione della politica | 2816 |
| Documento di policy JSON | 2816 |
| Ulteriori informazioni | 2817 |
| CloudWatchApplicationInsightsFullAccess | 2817 |
| Utilizzo di questa politica | 2817 |
| Dettagli della politica | 2817 |
| Versione della politica | 2817 |
| Documento di policy JSON | 2818 |
| Ulteriori informazioni | 2819 |
| CloudWatchApplicationInsightsReadOnlyAccess | 2819 |
| Utilizzo di questa politica | 2819 |
| Dettagli della politica | 2819 |
| Versione della politica | 2820 |
| Documento di policy JSON | 2820 |
| Ulteriori informazioni | 2820 |
| CloudwatchApplicationInsightsServiceLinkedRolePolicy | 2820 |
| Utilizzo di questa politica | 2821 |
| Dettagli della politica | 2821 |
| Versione della politica | 2821 |
| Documento di policy JSON | 2821 |
| Ulteriori informazioni | 2831 |

| | |
|---|------|
| CloudWatchApplicationSignalsFullAccess | 2831 |
| Utilizzo di questa politica | 2831 |
| Dettagli della politica | 2831 |
| Versione della politica | 2831 |
| Documento di policy JSON | 2832 |
| Ulteriori informazioni | 2834 |
| CloudWatchApplicationSignalsReadOnlyAccess | 2835 |
| Utilizzo di questa politica | 2835 |
| Dettagli della politica | 2835 |
| Versione della politica | 2835 |
| Documento di policy JSON | 2835 |
| Ulteriori informazioni | 2837 |
| CloudWatchApplicationSignalsServiceRolePolicy | 2838 |
| Utilizzo di questa politica | 2838 |
| Dettagli della politica | 2838 |
| Versione della politica | 2838 |
| Documento di policy JSON | 2838 |
| Ulteriori informazioni | 2841 |
| CloudWatchAutomaticDashboardsAccess | 2841 |
| Utilizzo di questa politica | 2841 |
| Dettagli della politica | 2841 |
| Versione della politica | 2841 |
| Documento di policy JSON | 2841 |
| Ulteriori informazioni | 2843 |
| CloudWatchCrossAccountSharingConfiguration | 2843 |
| Utilizzo di questa politica | 2843 |
| Dettagli della politica | 2843 |
| Versione della politica | 2843 |
| Documento di policy JSON | 2844 |
| Ulteriori informazioni | 2845 |
| CloudWatchEventsBuiltInTargetExecutionAccess | 2845 |
| Utilizzo di questa politica | 2845 |
| Dettagli della politica | 2845 |
| Versione della politica | 2845 |
| Documento di policy JSON | 2846 |
| Ulteriori informazioni | 2846 |

| | |
|---|------|
| CloudWatchEventsFullAccess | 2846 |
| Utilizzo di questa politica | 2846 |
| Dettagli della politica | 2846 |
| Versione della politica | 2847 |
| Documento di policy JSON | 2847 |
| Ulteriori informazioni | 2849 |
| CloudWatchEventsInvocationAccess | 2849 |
| Utilizzo di questa politica | 2849 |
| Dettagli della politica | 2849 |
| Versione della politica | 2850 |
| Documento di policy JSON | 2850 |
| Ulteriori informazioni | 2850 |
| CloudWatchEventsReadOnlyAccess | 2850 |
| Utilizzo di questa politica | 2850 |
| Dettagli della politica | 2851 |
| Versione della politica | 2851 |
| Documento di policy JSON | 2851 |
| Ulteriori informazioni | 2852 |
| CloudWatchEventsServiceRolePolicy | 2853 |
| Utilizzo di questa politica | 2853 |
| Dettagli della politica | 2853 |
| Versione della politica | 2853 |
| Documento di policy JSON | 2853 |
| Ulteriori informazioni | 2854 |
| CloudWatchFullAccess | 2854 |
| Utilizzo di questa politica | 2854 |
| Dettagli della politica | 2854 |
| Versione della politica | 2854 |
| Documento di policy JSON | 2855 |
| Ulteriori informazioni | 2856 |
| CloudWatchFullAccessV2 | 2856 |
| Utilizzo di questa politica | 2856 |
| Dettagli della politica | 2856 |
| Versione della politica | 2856 |
| Documento di policy JSON | 2856 |
| Ulteriori informazioni | 2858 |

| | |
|--|------|
| CloudWatchInternetMonitorServiceRolePolicy | 2858 |
| Utilizzo di questa politica | 2858 |
| Dettagli della politica | 2859 |
| Versione della politica | 2859 |
| Documento di policy JSON | 2859 |
| Ulteriori informazioni | 2860 |
| CloudWatchLambdaInsightsExecutionRolePolicy | 2860 |
| Utilizzo di questa politica | 2860 |
| Dettagli della politica | 2860 |
| Versione della politica | 2861 |
| Documento di policy JSON | 2861 |
| Ulteriori informazioni | 2861 |
| CloudWatchLogsCrossAccountSharingConfiguration | 2862 |
| Utilizzo di questa politica | 2862 |
| Dettagli della politica | 2862 |
| Versione della politica | 2862 |
| Documento di policy JSON | 2862 |
| Ulteriori informazioni | 2863 |
| CloudWatchLogsFullAccess | 2863 |
| Utilizzo di questa politica | 2863 |
| Dettagli della politica | 2864 |
| Versione della politica | 2864 |
| Documento di policy JSON | 2864 |
| Ulteriori informazioni | 2864 |
| CloudWatchLogsReadOnlyAccess | 2865 |
| Utilizzo di questa politica | 2865 |
| Dettagli della politica | 2865 |
| Versione della politica | 2865 |
| Documento di policy JSON | 2865 |
| Ulteriori informazioni | 2866 |
| CloudWatchNetworkMonitorServiceRolePolicy | 2866 |
| Utilizzo di questa politica | 2866 |
| Dettagli della politica | 2866 |
| Versione della politica | 2867 |
| Documento di policy JSON | 2867 |
| Ulteriori informazioni | 2868 |

| | |
|--|------|
| CloudWatchReadOnlyAccess | 2868 |
| Utilizzo di questa politica | 2868 |
| Dettagli della politica | 2868 |
| Versione della politica | 2869 |
| Documento di policy JSON | 2869 |
| Ulteriori informazioni | 2870 |
| CloudWatchSyntheticsFullAccess | 2870 |
| Utilizzo di questa politica | 2870 |
| Dettagli della politica | 2871 |
| Versione della politica | 2871 |
| Documento di policy JSON | 2871 |
| Ulteriori informazioni | 2876 |
| CloudWatchSyntheticsReadOnlyAccess | 2876 |
| Utilizzo di questa politica | 2876 |
| Dettagli della politica | 2876 |
| Versione della politica | 2876 |
| Documento di policy JSON | 2876 |
| Ulteriori informazioni | 2877 |
| ComprehendDataAccessRolePolicy | 2877 |
| Utilizzo di questa politica | 2877 |
| Dettagli della politica | 2877 |
| Versione della politica | 2878 |
| Documento di policy JSON | 2878 |
| Ulteriori informazioni | 2878 |
| ComprehendFullAccess | 2878 |
| Utilizzo di questa politica | 2879 |
| Dettagli della politica | 2879 |
| Versione della politica | 2879 |
| Documento di policy JSON | 2879 |
| Ulteriori informazioni | 2880 |
| ComprehendMedicalFullAccess | 2880 |
| Utilizzo di questa politica | 2880 |
| Dettagli della politica | 2880 |
| Versione della politica | 2880 |
| Documento di policy JSON | 2880 |
| Ulteriori informazioni | 2881 |

| | |
|---|------|
| ComprehendReadOnly | 2881 |
| Utilizzo di questa politica | 2881 |
| Dettagli della politica | 2881 |
| Versione della politica | 2881 |
| Documento di policy JSON | 2882 |
| Ulteriori informazioni | 2883 |
| ComputeOptimizerReadOnlyAccess | 2883 |
| Utilizzo di questa politica | 2883 |
| Dettagli della politica | 2883 |
| Versione della politica | 2884 |
| Documento di policy JSON | 2884 |
| Ulteriori informazioni | 2885 |
| ComputeOptimizerServiceRolePolicy | 2885 |
| Utilizzo di questa politica | 2885 |
| Dettagli della politica | 2885 |
| Versione della politica | 2885 |
| Documento di policy JSON | 2886 |
| Ulteriori informazioni | 2887 |
| ConfigConformsServiceRolePolicy | 2887 |
| Utilizzo di questa politica | 2887 |
| Dettagli della politica | 2887 |
| Versione della politica | 2888 |
| Documento di policy JSON | 2888 |
| Ulteriori informazioni | 2890 |
| CostOptimizationHubAdminAccess | 2891 |
| Utilizzo di questa politica | 2891 |
| Dettagli della politica | 2891 |
| Versione della politica | 2891 |
| Documento di policy JSON | 2891 |
| Ulteriori informazioni | 2893 |
| CostOptimizationHubReadOnlyAccess | 2893 |
| Utilizzo di questa politica | 2893 |
| Dettagli della politica | 2893 |
| Versione della politica | 2893 |
| Documento di policy JSON | 2893 |
| Ulteriori informazioni | 2894 |

| | |
|--|------|
| CostOptimizationHubServiceRolePolicy | 2894 |
| Utilizzo di questa politica | 2894 |
| Dettagli della politica | 2894 |
| Versione della politica | 2895 |
| Documento di policy JSON | 2895 |
| Ulteriori informazioni | 2896 |
| CustomerProfilesServiceLinkedRolePolicy | 2896 |
| Utilizzo di questa politica | 2896 |
| Dettagli della politica | 2896 |
| Versione della politica | 2896 |
| Documento di policy JSON | 2897 |
| Ulteriori informazioni | 2897 |
| DatabaseAdministrator | 2897 |
| Utilizzo di questa politica | 2898 |
| Dettagli della politica | 2898 |
| Versione della politica | 2898 |
| Documento di policy JSON | 2898 |
| Ulteriori informazioni | 2900 |
| DataScientist | 2901 |
| Utilizzo di questa politica | 2901 |
| Dettagli della politica | 2901 |
| Versione della politica | 2901 |
| Documento di policy JSON | 2901 |
| Ulteriori informazioni | 2905 |
| DAXServiceRolePolicy | 2905 |
| Utilizzo di questa politica | 2905 |
| Dettagli della politica | 2905 |
| Versione della politica | 2906 |
| Documento di policy JSON | 2906 |
| Ulteriori informazioni | 2906 |
| DynamoDBCloudWatchContributorInsightsServiceRolePolicy | 2907 |
| Utilizzo di questa politica | 2907 |
| Dettagli della politica | 2907 |
| Versione della politica | 2907 |
| Documento di policy JSON | 2907 |
| Ulteriori informazioni | 2908 |

| | |
|---|------|
| DynamoDBKinesisReplicationServiceRolePolicy | 2908 |
| Utilizzo di questa politica | 2908 |
| Dettagli della politica | 2908 |
| Versione della politica | 2909 |
| Documento di policy JSON | 2909 |
| Ulteriori informazioni | 2909 |
| DynamoDBReplicationServiceRolePolicy | 2910 |
| Utilizzo di questa politica | 2910 |
| Dettagli della politica | 2910 |
| Versione della politica | 2910 |
| Documento di policy JSON | 2910 |
| Ulteriori informazioni | 2911 |
| EC2FastLaunchFullAccess | 2912 |
| Utilizzo di questa politica | 2912 |
| Dettagli della politica | 2912 |
| Versione della politica | 2912 |
| Documento di policy JSON | 2912 |
| Ulteriori informazioni | 2915 |
| EC2FastLaunchServiceRolePolicy | 2915 |
| Utilizzo di questa politica | 2915 |
| Dettagli della politica | 2915 |
| Versione della politica | 2916 |
| Documento di policy JSON | 2916 |
| Ulteriori informazioni | 2920 |
| EC2FleetTimeShiftableServiceRolePolicy | 2920 |
| Utilizzo di questa politica | 2920 |
| Dettagli della politica | 2920 |
| Versione della politica | 2920 |
| Documento di policy JSON | 2920 |
| Ulteriori informazioni | 2922 |
| Ec2ImageBuilderCrossAccountDistributionAccess | 2922 |
| Utilizzo di questa politica | 2922 |
| Dettagli della politica | 2922 |
| Versione della politica | 2922 |
| Documento di policy JSON | 2923 |
| Ulteriori informazioni | 2923 |

| | |
|---|------|
| EC2ImageBuilderLifecycleExecutionPolicy | 2923 |
| Utilizzo di questa politica | 2924 |
| Dettagli della politica | 2924 |
| Versione della politica | 2924 |
| Documento di policy JSON | 2924 |
| Ulteriori informazioni | 2926 |
| EC2InstanceConnect | 2926 |
| Utilizzo di questa politica | 2926 |
| Dettagli della politica | 2927 |
| Versione della politica | 2927 |
| Documento di policy JSON | 2927 |
| Ulteriori informazioni | 2927 |
| Ec2InstanceConnectEndpoint | 2928 |
| Utilizzo di questa politica | 2928 |
| Dettagli della politica | 2928 |
| Versione della politica | 2928 |
| Documento di policy JSON | 2928 |
| Ulteriori informazioni | 2930 |
| EC2InstanceProfileForImageBuilder | 2930 |
| Utilizzo di questa politica | 2931 |
| Dettagli della politica | 2931 |
| Versione della politica | 2931 |
| Documento di policy JSON | 2931 |
| Ulteriori informazioni | 2932 |
| EC2InstanceProfileForImageBuilderECRContainerBuilds | 2932 |
| Utilizzo di questa politica | 2933 |
| Dettagli della politica | 2933 |
| Versione della politica | 2933 |
| Documento di policy JSON | 2933 |
| Ulteriori informazioni | 2934 |
| ECRReplicationServiceRolePolicy | 2935 |
| Utilizzo di questa politica | 2935 |
| Dettagli della politica | 2935 |
| Versione della politica | 2935 |
| Documento di policy JSON | 2935 |
| Ulteriori informazioni | 2936 |

| | |
|--|------|
| ElastiCacheServiceRolePolicy | 2936 |
| Utilizzo di questa politica | 2936 |
| Dettagli della politica | 2936 |
| Versione della politica | 2936 |
| Documento di policy JSON | 2937 |
| Ulteriori informazioni | 2938 |
| ElasticLoadBalancingFullAccess | 2939 |
| Utilizzo di questa politica | 2939 |
| Dettagli della politica | 2939 |
| Versione della politica | 2939 |
| Documento di policy JSON | 2939 |
| Ulteriori informazioni | 2941 |
| ElasticLoadBalancingReadOnly | 2941 |
| Utilizzo di questa politica | 2941 |
| Dettagli della politica | 2941 |
| Versione della politica | 2941 |
| Documento di policy JSON | 2941 |
| Ulteriori informazioni | 2942 |
| ElementalActivationsDownloadSoftwareAccess | 2943 |
| Utilizzo di questa politica | 2943 |
| Dettagli della politica | 2943 |
| Versione della politica | 2943 |
| Documento di policy JSON | 2943 |
| Ulteriori informazioni | 2944 |
| ElementalActivationsFullAccess | 2944 |
| Utilizzo di questa politica | 2944 |
| Dettagli della politica | 2944 |
| Versione della politica | 2944 |
| Documento di policy JSON | 2945 |
| Ulteriori informazioni | 2945 |
| ElementalActivationsGenerateLicenses | 2945 |
| Utilizzo di questa politica | 2945 |
| Dettagli della politica | 2945 |
| Versione della politica | 2946 |
| Documento di policy JSON | 2946 |
| Ulteriori informazioni | 2946 |

| | |
|---|------|
| ElementalActivationsReadOnlyAccess | 2947 |
| Utilizzo di questa politica | 2947 |
| Dettagli della politica | 2947 |
| Versione della politica | 2947 |
| Documento di policy JSON | 2947 |
| Ulteriori informazioni | 2948 |
| ElementalAppliancesSoftwareFullAccess | 2948 |
| Utilizzo di questa politica | 2948 |
| Dettagli della politica | 2948 |
| Versione della politica | 2948 |
| Documento di policy JSON | 2949 |
| Ulteriori informazioni | 2949 |
| ElementalAppliancesSoftwareReadOnlyAccess | 2949 |
| Utilizzo di questa politica | 2949 |
| Dettagli della politica | 2949 |
| Versione della politica | 2950 |
| Documento di policy JSON | 2950 |
| Ulteriori informazioni | 2950 |
| ElementalSupportCenterFullAccess | 2950 |
| Utilizzo di questa politica | 2951 |
| Dettagli della politica | 2951 |
| Versione della politica | 2951 |
| Documento di policy JSON | 2951 |
| Ulteriori informazioni | 2951 |
| EMRDescribeClusterPolicyForEMRWAL | 2952 |
| Utilizzo di questa politica | 2952 |
| Dettagli della politica | 2952 |
| Versione della politica | 2952 |
| Documento di policy JSON | 2952 |
| Ulteriori informazioni | 2953 |
| FMSServiceRolePolicy | 2953 |
| Utilizzo di questa politica | 2953 |
| Dettagli della politica | 2953 |
| Versione della politica | 2953 |
| Documento di policy JSON | 2954 |
| Ulteriori informazioni | 2970 |

| | |
|---|------|
| FSxDeleteServiceLinkedRoleAccess | 2970 |
| Utilizzo di questa politica | 2970 |
| Dettagli della politica | 2970 |
| Versione della politica | 2970 |
| Documento di policy JSON | 2971 |
| Ulteriori informazioni | 2971 |
| GameLiftGameServerGroupPolicy | 2971 |
| Utilizzo di questa politica | 2971 |
| Dettagli della politica | 2971 |
| Versione della politica | 2972 |
| Documento di policy JSON | 2972 |
| Ulteriori informazioni | 2973 |
| GlobalAcceleratorFullAccess | 2974 |
| Utilizzo di questa politica | 2974 |
| Dettagli della politica | 2974 |
| Versione della politica | 2974 |
| Documento di policy JSON | 2974 |
| Ulteriori informazioni | 2975 |
| GlobalAcceleratorReadOnlyAccess | 2975 |
| Utilizzo di questa politica | 2976 |
| Dettagli della politica | 2976 |
| Versione della politica | 2976 |
| Documento di policy JSON | 2976 |
| Ulteriori informazioni | 2976 |
| GreengrassOTAUpdateArtifactAccess | 2977 |
| Utilizzo di questa politica | 2977 |
| Dettagli della politica | 2977 |
| Versione della politica | 2977 |
| Documento di policy JSON | 2977 |
| Ulteriori informazioni | 2978 |
| GroundTruthSyntheticConsoleFullAccess | 2978 |
| Utilizzo di questa politica | 2978 |
| Dettagli della politica | 2978 |
| Versione della politica | 2978 |
| Documento di policy JSON | 2979 |
| Ulteriori informazioni | 2979 |

| | |
|---|------|
| GroundTruthSyntheticConsoleReadOnlyAccess | 2979 |
| Utilizzo di questa politica | 2979 |
| Dettagli della politica | 2980 |
| Versione della politica | 2980 |
| Documento di policy JSON | 2980 |
| Ulteriori informazioni | 2980 |
| Health_OrganizationsServiceRolePolicy | 2981 |
| Utilizzo di questa politica | 2981 |
| Dettagli della politica | 2981 |
| Versione della politica | 2981 |
| Documento di policy JSON | 2981 |
| Ulteriori informazioni | 2982 |
| IAMAccessAdvisorReadOnly | 2982 |
| Utilizzo di questa politica | 2982 |
| Dettagli della politica | 2982 |
| Versione della politica | 2982 |
| Documento di policy JSON | 2983 |
| Ulteriori informazioni | 2983 |
| IAMAccessAnalyzerFullAccess | 2984 |
| Utilizzo di questa politica | 2984 |
| Dettagli della politica | 2984 |
| Versione della politica | 2984 |
| Documento di policy JSON | 2984 |
| Ulteriori informazioni | 2985 |
| IAMAccessAnalyzerReadOnlyAccess | 2985 |
| Utilizzo di questa politica | 2986 |
| Dettagli della politica | 2986 |
| Versione della politica | 2986 |
| Documento di policy JSON | 2986 |
| Ulteriori informazioni | 2987 |
| IAMFullAccess | 2987 |
| Utilizzo di questa politica | 2987 |
| Dettagli della politica | 2987 |
| Versione della politica | 2987 |
| Documento di policy JSON | 2987 |
| Ulteriori informazioni | 2988 |

| | |
|---|------|
| IAMReadOnlyAccess | 2988 |
| Utilizzo di questa politica | 2988 |
| Dettagli della politica | 2988 |
| Versione della politica | 2989 |
| Documento di policy JSON | 2989 |
| Ulteriori informazioni | 2989 |
| IAMSelfManageServiceSpecificCredentials | 2990 |
| Utilizzo di questa politica | 2990 |
| Dettagli della politica | 2990 |
| Versione della politica | 2990 |
| Documento di policy JSON | 2990 |
| Ulteriori informazioni | 2991 |
| IAMUserChangePassword | 2991 |
| Utilizzo di questa politica | 2991 |
| Dettagli della politica | 2991 |
| Versione della politica | 2991 |
| Documento di policy JSON | 2992 |
| Ulteriori informazioni | 2992 |
| IAMUserSSHKeys | 2992 |
| Utilizzo di questa politica | 2992 |
| Dettagli della politica | 2993 |
| Versione della politica | 2993 |
| Documento di policy JSON | 2993 |
| Ulteriori informazioni | 2993 |
| IVSFullAccess | 2994 |
| Utilizzo di questa politica | 2994 |
| Dettagli della politica | 2994 |
| Versione della politica | 2994 |
| Documento di policy JSON | 2994 |
| Ulteriori informazioni | 2995 |
| IVSReadOnlyAccess | 2995 |
| Utilizzo di questa politica | 2995 |
| Dettagli della politica | 2995 |
| Versione della politica | 2995 |
| Documento di policy JSON | 2996 |
| Ulteriori informazioni | 2997 |

| | |
|--|------|
| IVSRecordToS3 | 2997 |
| Utilizzo di questa politica | 2997 |
| Dettagli della politica | 2997 |
| Versione della politica | 2997 |
| Documento di policy JSON | 2998 |
| Ulteriori informazioni | 2998 |
| KafkaConnectServiceRolePolicy | 2998 |
| Utilizzo di questa politica | 2998 |
| Dettagli della politica | 2998 |
| Versione della politica | 2999 |
| Documento di policy JSON | 2999 |
| Ulteriori informazioni | 3000 |
| KafkaServiceRolePolicy | 3000 |
| Utilizzo di questa politica | 3001 |
| Dettagli della politica | 3001 |
| Versione della politica | 3001 |
| Documento di policy JSON | 3001 |
| Ulteriori informazioni | 3003 |
| KeyspacesReplicationServiceRolePolicy | 3003 |
| Utilizzo di questa politica | 3003 |
| Dettagli della politica | 3003 |
| Versione della politica | 3003 |
| Documento di policy JSON | 3003 |
| Ulteriori informazioni | 3004 |
| LakeFormationDataAccessServiceRolePolicy | 3004 |
| Utilizzo di questa politica | 3004 |
| Dettagli della politica | 3004 |
| Versione della politica | 3005 |
| Documento di policy JSON | 3005 |
| Ulteriori informazioni | 3005 |
| LexBotPolicy | 3005 |
| Utilizzo di questa politica | 3006 |
| Dettagli della politica | 3006 |
| Versione della politica | 3006 |
| Documento di policy JSON | 3006 |
| Ulteriori informazioni | 3007 |

| | |
|--|------|
| LexChannelPolicy | 3007 |
| Utilizzo di questa politica | 3007 |
| Dettagli della politica | 3007 |
| Versione della politica | 3007 |
| Documento di policy JSON | 3008 |
| Ulteriori informazioni | 3008 |
| LightsailExportAccess | 3008 |
| Utilizzo di questa politica | 3008 |
| Dettagli della politica | 3008 |
| Versione della politica | 3009 |
| Documento di policy JSON | 3009 |
| Ulteriori informazioni | 3010 |
| MediaConnectGatewayInstanceRolePolicy | 3010 |
| Utilizzo di questa politica | 3010 |
| Dettagli della politica | 3010 |
| Versione della politica | 3010 |
| Documento di policy JSON | 3010 |
| Ulteriori informazioni | 3011 |
| MediaPackageServiceRolePolicy | 3011 |
| Utilizzo di questa politica | 3011 |
| Dettagli della politica | 3011 |
| Versione della politica | 3012 |
| Documento di policy JSON | 3012 |
| Ulteriori informazioni | 3012 |
| MemoryDBServiceRolePolicy | 3012 |
| Utilizzo di questa politica | 3013 |
| Dettagli della politica | 3013 |
| Versione della politica | 3013 |
| Documento di policy JSON | 3013 |
| Ulteriori informazioni | 3015 |
| MigrationHubDMSAccessServiceRolePolicy | 3015 |
| Utilizzo di questa politica | 3015 |
| Dettagli della politica | 3015 |
| Versione della politica | 3016 |
| Documento di policy JSON | 3016 |
| Ulteriori informazioni | 3017 |

| | |
|--|------|
| MigrationHubServiceRolePolicy | 3017 |
| Utilizzo di questa politica | 3017 |
| Dettagli della politica | 3017 |
| Versione della politica | 3017 |
| Documento di policy JSON | 3018 |
| Ulteriori informazioni | 3019 |
| MigrationHubSMSAccessServiceRolePolicy | 3019 |
| Utilizzo di questa politica | 3019 |
| Dettagli della politica | 3019 |
| Versione della politica | 3020 |
| Documento di policy JSON | 3020 |
| Ulteriori informazioni | 3021 |
| MonitronServiceRolePolicy | 3021 |
| Utilizzo di questa politica | 3021 |
| Dettagli della politica | 3021 |
| Versione della politica | 3021 |
| Documento di policy JSON | 3022 |
| Ulteriori informazioni | 3022 |
| NeptuneConsoleFullAccess | 3022 |
| Utilizzo di questa politica | 3022 |
| Dettagli della politica | 3023 |
| Versione della politica | 3023 |
| Documento di policy JSON | 3023 |
| Ulteriori informazioni | 3028 |
| NeptuneFullAccess | 3029 |
| Utilizzo di questa politica | 3029 |
| Dettagli della politica | 3029 |
| Versione della politica | 3029 |
| Documento di policy JSON | 3029 |
| Ulteriori informazioni | 3033 |
| NeptuneGraphReadOnlyAccess | 3033 |
| Utilizzo di questa politica | 3034 |
| Dettagli della politica | 3034 |
| Versione della politica | 3034 |
| Documento di policy JSON | 3034 |
| Ulteriori informazioni | 3036 |

| | |
|--|------|
| NeptuneReadOnlyAccess | 3036 |
| Utilizzo di questa politica | 3036 |
| Dettagli della politica | 3036 |
| Versione della politica | 3036 |
| Documento di policy JSON | 3036 |
| Ulteriori informazioni | 3039 |
| NetworkAdministrator | 3039 |
| Utilizzo di questa politica | 3039 |
| Dettagli della politica | 3039 |
| Versione della politica | 3039 |
| Documento di policy JSON | 3040 |
| Ulteriori informazioni | 3046 |
| OAMFullAccess | 3046 |
| Utilizzo di questa politica | 3046 |
| Dettagli della politica | 3047 |
| Versione della politica | 3047 |
| Documento di policy JSON | 3047 |
| Ulteriori informazioni | 3047 |
| OAMReadOnlyAccess | 3048 |
| Utilizzo di questa politica | 3048 |
| Dettagli della politica | 3048 |
| Versione della politica | 3048 |
| Documento di policy JSON | 3048 |
| Ulteriori informazioni | 3049 |
| OpensearchIngestionSelfManagedVpcePolicy | 3049 |
| Utilizzo di questa politica | 3049 |
| Dettagli della politica | 3049 |
| Versione della politica | 3049 |
| Documento di policy JSON | 3050 |
| Ulteriori informazioni | 3050 |
| PartnerCentralAccountManagementUserRoleAssociation | 3050 |
| Utilizzo di questa politica | 3051 |
| Dettagli della politica | 3051 |
| Versione della politica | 3051 |
| Documento di policy JSON | 3051 |
| Ulteriori informazioni | 3052 |

| | |
|---|------|
| PowerUserAccess | 3052 |
| Utilizzo di questa politica | 3052 |
| Dettagli della politica | 3052 |
| Versione della politica | 3053 |
| Documento di policy JSON | 3053 |
| Ulteriori informazioni | 3053 |
| QBusinessServiceRolePolicy | 3054 |
| Utilizzo di questa politica | 3054 |
| Dettagli della politica | 3054 |
| Versione della politica | 3054 |
| Documento di policy JSON | 3054 |
| Ulteriori informazioni | 3056 |
| QuickSightAccessForS3StorageManagementAnalyticsReadOnly | 3056 |
| Utilizzo di questa politica | 3056 |
| Dettagli della politica | 3056 |
| Versione della politica | 3057 |
| Documento di policy JSON | 3057 |
| Ulteriori informazioni | 3057 |
| RDSCloudHsmAuthorizationRole | 3058 |
| Utilizzo di questa politica | 3058 |
| Dettagli della politica | 3058 |
| Versione della politica | 3058 |
| Documento di policy JSON | 3058 |
| Ulteriori informazioni | 3059 |
| ReadOnlyAccess | 3059 |
| Utilizzo di questa politica | 3059 |
| Dettagli della politica | 3059 |
| Versione della politica | 3059 |
| Documento di policy JSON | 3060 |
| Ulteriori informazioni | 3109 |
| ResourceGroupsandTagEditorFullAccess | 3109 |
| Utilizzo di questa politica | 3109 |
| Dettagli della politica | 3109 |
| Versione della politica | 3110 |
| Documento di policy JSON | 3110 |
| Ulteriori informazioni | 3110 |

| | |
|--|------|
| ResourceGroupsandTagEditorReadOnlyAccess | 3111 |
| Utilizzo di questa politica | 3111 |
| Dettagli della politica | 3111 |
| Versione della politica | 3111 |
| Documento di policy JSON | 3111 |
| Ulteriori informazioni | 3112 |
| ResourceGroupsServiceRolePolicy | 3112 |
| Utilizzo di questa politica | 3112 |
| Dettagli della politica | 3112 |
| Versione della politica | 3113 |
| Documento di policy JSON | 3113 |
| Ulteriori informazioni | 3113 |
| ROSAAmazonEBSCSIDriverOperatorPolicy | 3113 |
| Utilizzo di questa politica | 3114 |
| Dettagli della politica | 3114 |
| Versione della politica | 3114 |
| Documento di policy JSON | 3114 |
| Ulteriori informazioni | 3117 |
| ROSACloudNetworkConfigOperatorPolicy | 3117 |
| Utilizzo di questa politica | 3117 |
| Dettagli della politica | 3118 |
| Versione della politica | 3118 |
| Documento di policy JSON | 3118 |
| Ulteriori informazioni | 3119 |
| ROSAControlPlaneOperatorPolicy | 3119 |
| Utilizzo di questa politica | 3119 |
| Dettagli della politica | 3119 |
| Versione della politica | 3120 |
| Documento di policy JSON | 3120 |
| Ulteriori informazioni | 3124 |
| ROSAImageRegistryOperatorPolicy | 3124 |
| Utilizzo di questa politica | 3125 |
| Dettagli della politica | 3125 |
| Versione della politica | 3125 |
| Documento di policy JSON | 3125 |
| Ulteriori informazioni | 3126 |

| | |
|------------------------------------|------|
| ROSAIngressOperatorPolicy | 3127 |
| Utilizzo di questa politica | 3127 |
| Dettagli della politica | 3127 |
| Versione della politica | 3127 |
| Documento di policy JSON | 3127 |
| Ulteriori informazioni | 3128 |
| ROSAInstallerPolicy | 3128 |
| Utilizzo di questa politica | 3128 |
| Dettagli della politica | 3129 |
| Versione della politica | 3129 |
| Documento di policy JSON | 3129 |
| Ulteriori informazioni | 3137 |
| ROSAKMSPProviderPolicy | 3137 |
| Utilizzo di questa politica | 3137 |
| Dettagli della politica | 3137 |
| Versione della politica | 3138 |
| Documento di policy JSON | 3138 |
| Ulteriori informazioni | 3138 |
| ROSAKubeControllerPolicy | 3139 |
| Utilizzo di questa politica | 3139 |
| Dettagli della politica | 3139 |
| Versione della politica | 3139 |
| Documento di policy JSON | 3139 |
| Ulteriori informazioni | 3144 |
| ROSAManageSubscription | 3144 |
| Utilizzo di questa politica | 3144 |
| Dettagli della politica | 3144 |
| Versione della politica | 3144 |
| Documento di policy JSON | 3144 |
| Ulteriori informazioni | 3145 |
| ROSANodePoolManagementPolicy | 3145 |
| Utilizzo di questa politica | 3146 |
| Dettagli della politica | 3146 |
| Versione della politica | 3146 |
| Documento di policy JSON | 3146 |
| Ulteriori informazioni | 3152 |

| | |
|---|------|
| ROSASRESupportPolicy | 3152 |
| Utilizzo di questa politica | 3152 |
| Dettagli della politica | 3152 |
| Versione della politica | 3152 |
| Documento di policy JSON | 3153 |
| Ulteriori informazioni | 3157 |
| ROSAWorkerInstancePolicy | 3158 |
| Utilizzo di questa politica | 3158 |
| Dettagli della politica | 3158 |
| Versione della politica | 3158 |
| Documento di policy JSON | 3158 |
| Ulteriori informazioni | 3159 |
| Route53RecoveryReadinessServiceRolePolicy | 3159 |
| Utilizzo di questa politica | 3159 |
| Dettagli della politica | 3159 |
| Versione della politica | 3159 |
| Documento di policy JSON | 3160 |
| Ulteriori informazioni | 3163 |
| Route53ResolverServiceRolePolicy | 3163 |
| Utilizzo di questa politica | 3163 |
| Dettagli della politica | 3164 |
| Versione della politica | 3164 |
| Documento di policy JSON | 3164 |
| Ulteriori informazioni | 3165 |
| S3StorageLensServiceRolePolicy | 3165 |
| Utilizzo di questa politica | 3165 |
| Dettagli della politica | 3165 |
| Versione della politica | 3165 |
| Documento di policy JSON | 3165 |
| Ulteriori informazioni | 3166 |
| SecretsManagerReadWrite | 3166 |
| Utilizzo di questa politica | 3166 |
| Dettagli della politica | 3166 |
| Versione della politica | 3167 |
| Documento di policy JSON | 3167 |
| Ulteriori informazioni | 3168 |

| | |
|---|------|
| SecurityAudit | 3169 |
| Utilizzo di questa politica | 3169 |
| Dettagli della politica | 3169 |
| Versione della politica | 3169 |
| Documento di policy JSON | 3169 |
| Ulteriori informazioni | 3186 |
| SecurityLakeServiceLinkedRole | 3187 |
| Utilizzo di questa politica | 3187 |
| Dettagli della politica | 3187 |
| Versione della politica | 3187 |
| Documento di policy JSON | 3187 |
| Ulteriori informazioni | 3190 |
| ServerMigration_ServiceRole | 3190 |
| Utilizzo di questa politica | 3190 |
| Dettagli della politica | 3190 |
| Versione della politica | 3191 |
| Documento di policy JSON | 3191 |
| Ulteriori informazioni | 3196 |
| ServerMigrationConnector | 3196 |
| Utilizzo di questa politica | 3196 |
| Dettagli della politica | 3196 |
| Versione della politica | 3196 |
| Documento di policy JSON | 3197 |
| Ulteriori informazioni | 3198 |
| ServerMigrationServiceConsoleFullAccess | 3198 |
| Utilizzo di questa politica | 3198 |
| Dettagli della politica | 3198 |
| Versione della politica | 3199 |
| Documento di policy JSON | 3199 |
| Ulteriori informazioni | 3200 |
| ServerMigrationServiceLaunchRole | 3201 |
| Utilizzo di questa politica | 3201 |
| Dettagli della politica | 3201 |
| Versione della politica | 3201 |
| Documento di policy JSON | 3201 |
| Ulteriori informazioni | 3204 |

| | |
|---|------|
| ServerMigrationServiceRoleForInstanceValidation | 3204 |
| Utilizzo di questa politica | 3204 |
| Dettagli della politica | 3205 |
| Versione della politica | 3205 |
| Documento di policy JSON | 3205 |
| Ulteriori informazioni | 3205 |
| ServiceQuotasFullAccess | 3206 |
| Utilizzo di questa politica | 3206 |
| Dettagli della politica | 3206 |
| Versione della politica | 3206 |
| Documento di policy JSON | 3206 |
| Ulteriori informazioni | 3208 |
| ServiceQuotasReadOnlyAccess | 3208 |
| Utilizzo di questa politica | 3208 |
| Dettagli della politica | 3208 |
| Versione della politica | 3209 |
| Documento di policy JSON | 3209 |
| Ulteriori informazioni | 3210 |
| ServiceQuotasServiceRolePolicy | 3210 |
| Utilizzo di questa politica | 3210 |
| Dettagli della politica | 3210 |
| Versione della politica | 3210 |
| Documento di policy JSON | 3211 |
| Ulteriori informazioni | 3211 |
| SimpleWorkflowFullAccess | 3211 |
| Utilizzo di questa politica | 3211 |
| Dettagli della politica | 3211 |
| Versione della politica | 3212 |
| Documento di policy JSON | 3212 |
| Ulteriori informazioni | 3212 |
| SplitCostAllocationDataServiceRolePolicy | 3212 |
| Utilizzo di questa politica | 3213 |
| Dettagli della politica | 3213 |
| Versione della politica | 3213 |
| Documento di policy JSON | 3213 |
| Ulteriori informazioni | 3214 |

| | |
|---|------|
| SupportUser | 3214 |
| Utilizzo di questa politica | 3214 |
| Dettagli della politica | 3214 |
| Versione della politica | 3214 |
| Documento di policy JSON | 3215 |
| Ulteriori informazioni | 3220 |
| SystemAdministrator | 3220 |
| Utilizzo di questa politica | 3220 |
| Dettagli della politica | 3220 |
| Versione della politica | 3220 |
| Documento di policy JSON | 3220 |
| Ulteriori informazioni | 3226 |
| TranslateFullAccess | 3227 |
| Utilizzo di questa politica | 3227 |
| Dettagli della politica | 3227 |
| Versione della politica | 3227 |
| Documento di policy JSON | 3227 |
| Ulteriori informazioni | 3228 |
| TranslateReadOnly | 3228 |
| Utilizzo di questa politica | 3228 |
| Dettagli della politica | 3228 |
| Versione della politica | 3228 |
| Documento di policy JSON | 3229 |
| Ulteriori informazioni | 3229 |
| ViewOnlyAccess | 3230 |
| Utilizzo di questa politica | 3230 |
| Dettagli della politica | 3230 |
| Versione della politica | 3230 |
| Documento di policy JSON | 3230 |
| Ulteriori informazioni | 3239 |
| VMImportExportRoleForAWSConnector | 3239 |
| Utilizzo di questa politica | 3239 |
| Dettagli della politica | 3239 |
| Versione della politica | 3240 |
| Documento di policy JSON | 3240 |
| Ulteriori informazioni | 3240 |

| | |
|---|------|
| VPCLatticeFullAccess | 3241 |
| Utilizzo di questa politica | 3241 |
| Dettagli della politica | 3241 |
| Versione della politica | 3241 |
| Documento di policy JSON | 3241 |
| Ulteriori informazioni | 3243 |
| VPCLatticeReadOnlyAccess | 3243 |
| Utilizzo di questa politica | 3244 |
| Dettagli della politica | 3244 |
| Versione della politica | 3244 |
| Documento di policy JSON | 3244 |
| Ulteriori informazioni | 3245 |
| VPCLatticeServicesInvokeAccess | 3245 |
| Utilizzo di questa politica | 3245 |
| Dettagli della politica | 3245 |
| Versione della politica | 3246 |
| Documento di policy JSON | 3246 |
| Ulteriori informazioni | 3246 |
| WAFLoggingServiceRolePolicy | 3246 |
| Utilizzo di questa politica | 3247 |
| Dettagli della politica | 3247 |
| Versione della politica | 3247 |
| Documento di policy JSON | 3247 |
| Ulteriori informazioni | 3248 |
| WAFRegionalLoggingServiceRolePolicy | 3248 |
| Utilizzo di questa politica | 3248 |
| Dettagli della politica | 3248 |
| Versione della politica | 3248 |
| Documento di policy JSON | 3248 |
| Ulteriori informazioni | 3249 |
| WAFV2LoggingServiceRolePolicy | 3249 |
| Utilizzo di questa politica | 3249 |
| Dettagli della politica | 3249 |
| Versione della politica | 3250 |
| Documento di policy JSON | 3250 |
| Ulteriori informazioni | 3250 |

| | |
|--|----------|
| WellArchitectedConsoleFullAccess | 3251 |
| Utilizzo di questa politica | 3251 |
| Dettagli della politica | 3251 |
| Versione della politica | 3251 |
| Documento di policy JSON | 3251 |
| Ulteriori informazioni | 3252 |
| WellArchitectedConsoleReadOnlyAccess | 3252 |
| Utilizzo di questa politica | 3252 |
| Dettagli della politica | 3252 |
| Versione della politica | 3252 |
| Documento di policy JSON | 3253 |
| Ulteriori informazioni | 3253 |
| WorkLinkServiceRolePolicy | 3253 |
| Utilizzo di questa politica | 3253 |
| Dettagli della politica | 3253 |
| Versione della politica | 3254 |
| Documento di policy JSON | 3254 |
| Ulteriori informazioni | 3254 |
| | mmmcclvi |

Cosa sono le policy AWS gestite?

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni. Ti consentono di iniziare ad assegnare le autorizzazioni a utenti, gruppi e ruoli più facilmente che se dovessi scrivere le politiche da solo.

Ricorda: le policy gestite di AWS potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché sono disponibili per l'uso da parte di tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWS aggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWS aggiorni una policy gestita da AWS quando viene avviato un nuovo servizio AWS o vengono rese disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta la pagina [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

Comprendere le pagine di riferimento delle politiche

Ogni pagina di riferimento sulle politiche include le seguenti informazioni:

- Utilizzo di questa politica: se è possibile allegare la politica a utenti, gruppi e ruoli
- Dettagli della politica
 - Tipo: il tipo di politica AWS gestita
 - `AWS managed policy`— Una politica AWS gestita standard
 - `Job function policy`— Politica in linea con le funzioni lavorative comuni del settore
 - `Service-linked role policy`— Policy associata a un ruolo collegato al servizio che consente a un servizio di eseguire azioni per conto dell'utente, ad esempio [the section called “AmazonRDSPreviewServiceRolePolicy”](#)
 - `Service role policy`— Politica progettata per funzionare con ruoli di servizio, come [the section called “AWSControlTowerServiceRolePolicy”](#)
 - Ora di creazione: quando la politica è stata creata per la prima volta
 - Ora di modifica: quando è stata modificata questa versione della politica

- ARN: il nome Amazon Resource della policy
- Versione della policy: la versione delle autorizzazioni concesse dalla policy
- Documento sulla politica JSON: la politica JSON
- Ulteriori informazioni: collegamenti alla documentazione relativa alle AWS politiche gestite

Policy gestite da AWS obsolete

AWS aggiorna regolarmente le politiche AWS gestite. Nella maggior parte dei casi, aggiungiamo autorizzazioni a una politica. Questo accade quando lanciamo un nuovo servizio o una nuova funzionalità. Per migliorare la sicurezza delle politiche AWS gestite, a volte riduciamo l'ambito delle politiche. Quando rimuoviamo le autorizzazioni da una policy, impostiamo la policy su uno stato obsoleto e ne rendiamo disponibile una nuova. Quando un servizio o una funzionalità sono AWS obsoleti, deprechiamo anche la policy gestita per quella funzionalità. AWS

Se ricevi una notifica via e-mail che indica che una politica che stai utilizzando è obsoleta, ti consigliamo di agire immediatamente. Identifica la modifica alla politica e aggiorna i flussi di lavoro. Se AWS fornisce una politica sostitutiva, pianifica di allegarla a tutte le identità interessate (utenti, gruppi e ruoli) e quindi scollegare la politica obsoleta da tali identità.

Una policy obsoleta presenta le seguenti caratteristiche:

- È stata rimossa da questa guida.
- Le autorizzazioni continuano a funzionare per tutte le identità attualmente associate.
- Negli account in cui la policy è associata a un'identità, viene visualizzata nell'elenco Policies della console IAM con un'icona di avviso accanto ad essa.
- Non può essere associata a nessuna nuova identità. Se lo si scollega da un'identità corrente, non è possibile ricollegarlo.
- Dopo averlo scollegato da tutte le entità correnti, non è più visibile.

AWS politiche gestite

AWS politiche gestite

- [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](#)
- [AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary](#)
- [AmazonDataZoneSageMakerManageAccessRolePolicy](#)
- [AmazonDataZoneSageMakerProvisioningRolePolicy](#)

- [AmazonDetectiveFullAccess](#)
- [AmazonDetectiveInvestigatorAccess](#)
- [AmazonDetectiveMemberAccess](#)
- [AmazonDetectiveOrganizationsAccess](#)
- [AmazonDetectiveServiceLinkedRolePolicy](#)
- [AmazonDevOpsGuruConsoleFullAccess](#)
- [AmazonDevOpsGuruFullAccess](#)
- [AmazonDevOpsGuruOrganizationsAccess](#)
- [AmazonDevOpsGuruReadOnlyAccess](#)
- [AmazonDevOpsGuruServiceRolePolicy](#)
- [AmazonDMSCloudWatchLogsRole](#)
- [AmazonDMSRedshiftS3Role](#)
- [AmazonDMSVPCManagementRole](#)
- [AmazonDocDB-ElasticServiceRolePolicy](#)
- [AmazonDocDBConsoleFullAccess](#)
- [AmazonDocDBElasticFullAccess](#)
- [AmazonDocDBElasticReadOnlyAccess](#)
- [AmazonDocDBFullAccess](#)
- [AmazonDocDBReadOnlyAccess](#)
- [AmazonDRSVPCManagement](#)
- [AmazonDynamoDBFullAccess](#)
- [AmazonDynamoDBFullAccesswithDataPipeline](#)
- [AmazonDynamoDBReadOnlyAccess](#)
- [AmazonEBSCSIDriverPolicy](#)
- [AmazonEC2ContainerRegistryFullAccess](#)
- [AmazonEC2ContainerRegistryPowerUser](#)
- [AmazonEC2ContainerRegistryReadOnly](#)
- [AmazonEC2ContainerServiceAutoscaleRole](#)
- [AmazonEC2ContainerServiceEventsRole](#)

- 7

- [AmazonElasticCacheReadOnlyAccess](#)
- [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](#)
- [AmazonOpenSearchDirectQueryGlueCreateAccess](#)
- [AmazonOpenSearchIngestionFullAccess](#)
- [AmazonOpenSearchIngestionReadOnlyAccess](#)
- [AmazonOpenSearchIngestionServiceRolePolicy](#)
- [AmazonOpenSearchServerlessServiceRolePolicy](#)
- [AmazonOpenSearchServiceCognitoAccess](#)
- [AmazonOpenSearchServiceFullAccess](#)
- [AmazonOpenSearchServiceReadOnlyAccess](#)
- [AmazonOpenSearchServiceRolePolicy](#)
- [AmazonPersonalizeFullAccess](#)
- [AmazonPollyFullAccess](#)
- [AmazonPollyReadOnlyAccess](#)
- [AmazonPrometheusConsoleFullAccess](#)
- [AmazonPrometheusFullAccess](#)
- [AmazonPrometheusQueryAccess](#)
- [AmazonPrometheusRemoteWriteAccess](#)
- [AmazonPrometheusScraperServiceRolePolicy](#)
- [AmazonQFullAccess](#)
- [AmazonQLDBConsoleFullAccess](#)
- [AmazonQLDBFullAccess](#)

- [AmazonQLDBReadOnly](#)
- [AmazonRDSBetaServiceRolePolicy](#)
- [AmazonRDSCustomInstanceProfileRolePolicy](#)
- [AmazonRDSCustomPreviewServiceRolePolicy](#)
- [AmazonRDSCustomServiceRolePolicy](#)
- [AmazonRDSDDataFullAccess](#)
- [AmazonRDSDirectoryServiceAccess](#)
- [AmazonRDSEnhancedMonitoringRole](#)
- [AmazonRDSFullAccess](#)
- [AmazonRDSPerformanceInsightsFullAccess](#)
- [AmazonRDSPerformanceInsightsReadOnly](#)
- [AmazonRDSPreviewServiceRolePolicy](#)
- [AmazonRDSReadOnlyAccess](#)
- [AmazonRDSServiceRolePolicy](#)
- [AmazonRedshiftAllCommandsFullAccess](#)
- [AmazonRedshiftDataFullAccess](#)
- [AmazonRedshiftFullAccess](#)
- [AmazonRedshiftQueryEditor](#)
- [AmazonRedshiftQueryEditorV2FullAccess](#)
- [AmazonRedshiftQueryEditorV2NoSharing](#)
- [AmazonRedshiftQueryEditorV2ReadSharing](#)
- [AmazonRedshiftQueryEditorV2ReadWriteSharing](#)
- [AmazonRedshiftReadOnlyAccess](#)
- [AmazonRedshiftServiceLinkedRolePolicy](#)
- [AmazonRekognitionCustomLabelsFullAccess](#)
- [AmazonRekognitionFullAccess](#)
- [AmazonRekognitionReadOnlyAccess](#)
- [AmazonRekognitionServiceRole](#)
- [AmazonRoute53AutoNamingFullAccess](#)

- [AmazonRoute53AutoNamingReadOnlyAccess](#)
- [AmazonRoute53AutoNamingRegistrantAccess](#)
- [AmazonRoute53DomainsFullAccess](#)
- [AmazonRoute53DomainsReadOnlyAccess](#)
- [AmazonRoute53FullAccess](#)
- [AmazonRoute53ProfilesFullAccess](#)
- [AmazonRoute53ProfilesReadOnlyAccess](#)
- [AmazonRoute53ReadOnlyAccess](#)
- [AmazonRoute53RecoveryClusterFullAccess](#)
- [AmazonRoute53RecoveryClusterReadOnlyAccess](#)
- [AmazonRoute53RecoveryControlConfigFullAccess](#)
- [AmazonRoute53RecoveryControlConfigReadOnlyAccess](#)
- [AmazonRoute53RecoveryReadinessFullAccess](#)
- [AmazonRoute53RecoveryReadinessReadOnlyAccess](#)
- [AmazonRoute53ResolverFullAccess](#)
- [AmazonRoute53ResolverReadOnlyAccess](#)
- [AmazonS3FullAccess](#)
- [AmazonS3ObjectLambdaExecutionRolePolicy](#)
- [AmazonS3OutpostsFullAccess](#)
- [AmazonS3OutpostsReadOnlyAccess](#)
- [AmazonS3ReadOnlyAccess](#)
- [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](#)

- [AmazonSESServiceRolePolicy](#)
- [AmazonSNSFullAccess](#)
- [AmazonSNSReadOnlyAccess](#)
- [AmazonSNSRole](#)
- [AmazonSQSFullAccess](#)
- [AmazonSQSReadOnlyAccess](#)
- [AmazonSSMAutomationApproverAccess](#)
- [AmazonSSMAutomationRole](#)
- [AmazonSSMDirectoryServiceAccess](#)
- [AmazonSSMFullAccess](#)
- [AmazonSSMMaintenanceWindowRole](#)
- [AmazonSSMManagedEC2InstanceDefaultPolicy](#)
- [AmazonSSMManagedInstanceCore](#)
- [AmazonSSMPatchAssociation](#)
- [AmazonSSMReadOnlyAccess](#)
- [AmazonSSMServiceRolePolicy](#)
- [AmazonSumerianFullAccess](#)
- [AmazonTextractFullAccess](#)
- [AmazonTextractServiceRole](#)
- [AmazonTimestreamConsoleFullAccess](#)
- [AmazonTimestreamFullAccess](#)
- [AmazonTimestreamInfluxDBFullAccess](#)
- [AmazonTimestreamInfluxDBServiceRolePolicy](#)
- [AmazonTimestreamReadOnlyAccess](#)
- [AmazonTranscribeFullAccess](#)
- [AmazonTranscribeReadOnlyAccess](#)
- [AmazonVPCCrossAccountNetworkInterfaceOperations](#)
- [AmazonVPCFullAccess](#)
- [AmazonVPCNetworkAccessAnalyzerFullAccessPolicy](#)

- [AmazonVPCReachabilityAnalyzerFullAccessPolicy](#)
- [AmazonVPCReachabilityAnalyzerPathComponentReadPolicy](#)
- [AmazonVPCReadOnlyAccess](#)
- [AmazonWorkDocsFullAccess](#)
- [AmazonWorkDocsReadOnlyAccess](#)
- [AmazonWorkMailEventsServiceRolePolicy](#)
- [AmazonWorkMailFullAccess](#)
- [AmazonWorkMailMessageFlowFullAccess](#)
- [AmazonWorkMailMessageFlowReadOnlyAccess](#)
- [AmazonWorkMailReadOnlyAccess](#)
- [AmazonWorkSpacesAdmin](#)
- [AmazonWorkSpacesApplicationManagerAdminAccess](#)
- [AmazonWorkspacesPCAAccess](#)
- [AmazonWorkSpacesSelfServiceAccess](#)
- [AmazonWorkSpacesServiceAccess](#)
- [AmazonWorkSpacesWebReadOnly](#)
- [AmazonWorkSpacesWebServiceRolePolicy](#)
- [AmazonZocaloFullAccess](#)
- [AmazonZocaloReadOnlyAccess](#)
- [AmplifyBackendDeployFullAccess](#)
- [APIGatewayServiceRolePolicy](#)
- [AppIntegrationsServiceLinkedRolePolicy](#)
- [ApplicationAutoScalingForAmazonAppStreamAccess](#)
- [ApplicationDiscoveryServiceContinuousExportServiceRolePolicy](#)
- [AppRunnerNetworkingServiceRolePolicy](#)
- [AppRunnerServiceRolePolicy](#)
- [AutoScalingConsoleFullAccess](#)
- [AutoScalingConsoleReadOnlyAccess](#)
- [AutoScalingFullAccess](#)

- [AutoScalingNotificationAccessRole](#)
- [AutoScalingReadOnlyAccess](#)
- [AutoScalingServiceRolePolicy](#)
- [AWS_ConfigRole](#)
- [AWSAccountActivityAccess](#)
- [AWSAccountManagementFullAccess](#)
- [AWSAccountManagementReadOnlyAccess](#)
- [AWSAccountUsageReportAccess](#)
- [AWSAgentlessDiscoveryService](#)
- [AWSAppFabricFullAccess](#)
- [AWSAppFabricReadOnlyAccess](#)
- [AWSAppFabricServiceRolePolicy](#)
- [AWSApplicationAutoscalingAppStreamFleetPolicy](#)
- [AWSApplicationAutoscalingCassandraTablePolicy](#)
- [AWSApplicationAutoscalingComprehendEndpointPolicy](#)
- [AWSApplicationAutoScalingCustomResourcePolicy](#)
- [AWSApplicationAutoscalingDynamoDBTablePolicy](#)
- [AWSApplicationAutoscalingEC2SpotFleetRequestPolicy](#)
- [AWSApplicationAutoscalingECSServicePolicy](#)
- [AWSApplicationAutoscalingElastiCacheRGPolicy](#)
- [AWSApplicationAutoscalingEMRInstanceGroupPolicy](#)
- [AWSApplicationAutoscalingKafkaClusterPolicy](#)
- [AWSApplicationAutoscalingLambdaConcurrencyPolicy](#)
- [AWSApplicationAutoscalingNeptuneClusterPolicy](#)
- [AWSApplicationAutoscalingRDSClusterPolicy](#)
- [AWSApplicationAutoscalingSageMakerEndpointPolicy](#)
- [AWSApplicationDiscoveryAgentAccess](#)
- [AWSApplicationDiscoveryAgentlessCollectorAccess](#)
- [AWSApplicationDiscoveryServiceFullAccess](#)

- [AWSApplicationMigrationAgentInstallationPolicy](#)
- [AWSApplicationMigrationAgentPolicy](#)
- [AWSApplicationMigrationAgentPolicy_v2](#)
- [AWSApplicationMigrationConversionServerPolicy](#)
- [AWSApplicationMigrationEC2Access](#)
- [AWSApplicationMigrationFullAccess](#)
- [AWSApplicationMigrationMGHAccess](#)
- [AWSApplicationMigrationReadOnlyAccess](#)
- [AWSApplicationMigrationReplicationServerPolicy](#)
- [AWSApplicationMigrationServiceEc2InstancePolicy](#)
- [AWSApplicationMigrationServiceRolePolicy](#)
- [AWSApplicationMigrationSSMAccess](#)
- [AWSApplicationMigrationVCenterClientPolicy](#)
- [AWSAppMeshEnvoyAccess](#)
- [AWSAppMeshFullAccess](#)
- [AWSAppMeshPreviewEnvoyAccess](#)
- [AWSAppMeshPreviewServiceRolePolicy](#)
- [AWSAppMeshReadOnly](#)
- [AWSAppMeshServiceRolePolicy](#)
- [AWSAppRunnerFullAccess](#)
- [AWSAppRunnerReadOnlyAccess](#)
- [AWSAppRunnerServicePolicyForECRAccess](#)
- [AWSAppSyncAdministrator](#)
- [AWSAppSyncInvokeFullAccess](#)
- [AWSAppSyncPushToCloudWatchLogs](#)
- [AWSAppSyncSchemaAuthor](#)
- [AWSAppSyncServiceRolePolicy](#)
- [AWSArtifactAccountSync](#)
- [AWSArtifactReportsReadOnlyAccess](#)

- [AWSArtifactServiceRolePolicy](#)
- [AWSAuditManagerAdministratorAccess](#)
- [AWSAuditManagerServiceRolePolicy](#)
- [AWSAutoScalingPlansEC2AutoScalingPolicy](#)
- [AWSBackupAuditAccess](#)
- [AWSBackupDataTransferAccess](#)
- [AWSBackupFullAccess](#)
- [AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#)
- [AWSBackupOperatorAccess](#)
- [AWSBackupOrganizationAdminAccess](#)
- [AWSBackupRestoreAccessForSAPHANA](#)
- [AWSBackupServiceLinkedRolePolicyForBackup](#)
- [AWSBackupServiceLinkedRolePolicyForBackupTest](#)
- [AWSBackupServiceRolePolicyForBackup](#)
- [AWSBackupServiceRolePolicyForRestores](#)
- [AWSBackupServiceRolePolicyForS3Backup](#)
- [AWSBackupServiceRolePolicyForS3Restore](#)
- [AWSBatchFullAccess](#)
- [AWSBatchServiceEventTargetRole](#)
- [AWSBatchServiceRole](#)
- [AWSBCMDDataExportsServiceRolePolicy](#)
- [AWSBillingConductorFullAccess](#)
- [AWSBillingConductorReadOnlyAccess](#)
- [AWSBillingReadOnlyAccess](#)
- [AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM](#)
- [AWSBudgetsActionsWithAWSResourceControlAccess](#)
- [AWSBudgetsReadOnlyAccess](#)
- [AWSBugBustFullAccess](#)
- [AWSBugBustPlayerAccess](#)

- [AWSBugBustServiceRolePolicy](#)
- [AWSCertificateManagerFullAccess](#)
- [AWSCertificateManagerPrivateCAAuditor](#)
- [AWSCertificateManagerPrivateCAFullAccess](#)
- [AWSCertificateManagerPrivateCAPrivilegedUser](#)
- [AWSCertificateManagerPrivateCAReadOnly](#)
- [AWSCertificateManagerPrivateCAUser](#)
- [AWSCertificateManagerReadOnly](#)
- [AWSChatbotServiceLinkedRolePolicy](#)
- [AWSCleanRoomsFullAccess](#)
- [AWSCleanRoomsFullAccessNoQuerying](#)
- [AWSCleanRoomsMLFullAccess](#)
- [AWSCleanRoomsMLReadOnlyAccess](#)
- [AWSCleanRoomsReadOnlyAccess](#)
- [AWSCloud9Administrator](#)
- [AWSCloud9EnvironmentMember](#)
- [AWSCloud9ServiceRolePolicy](#)
- [AWSCloud9SSMInstanceProfile](#)
- [AWSCloud9User](#)
- [AWSCloudFormationFullAccess](#)
- [AWSCloudFormationReadOnlyAccess](#)
- [AWSCloudFrontLogger](#)
- [AWSCloudHSMFullAccess](#)
- [AWSCloudHSMReadOnlyAccess](#)
- [AWSCloudHSMRole](#)
- [AWSCloudMapDiscoverInstanceAccess](#)
- [AWSCloudMapFullAccess](#)
- [AWSCloudMapReadOnlyAccess](#)
- [AWSCloudMapRegisterInstanceAccess](#)

- [AWSCloudShellFullAccess](#)
- [AWSCloudTrail_FullAccess](#)
- [AWSCloudTrail_ReadOnlyAccess](#)
- [AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy](#)
- [AWSCodeArtifactAdminAccess](#)
- [AWSCodeArtifactReadOnlyAccess](#)
- [AWSCodeBuildAdminAccess](#)
- [AWSCodeBuildDeveloperAccess](#)
- [AWSCodeBuildReadOnlyAccess](#)
- [AWSCodeCommitFullAccess](#)
- [AWSCodeCommitPowerUser](#)
- [AWSCodeCommitReadOnly](#)
- [AWSCodeDeployDeployerAccess](#)
- [AWSCodeDeployFullAccess](#)
- [AWSCodeDeployReadOnlyAccess](#)
- [AWSCodeDeployRole](#)
- [AWSCodeDeployRoleForCloudFormation](#)
- [AWSCodeDeployRoleForECS](#)
- [AWSCodeDeployRoleForECSLimited](#)
- [AWSCodeDeployRoleForLambda](#)
- [AWSCodeDeployRoleForLambdaLimited](#)
- [AWSCodePipeline_FullAccess](#)
- [AWSCodePipeline_ReadOnlyAccess](#)
- [AWSCodePipelineApproverAccess](#)
- [AWSCodePipelineCustomActionAccess](#)
- [AWSCodeStarFullAccess](#)
- [AWSCodeStarNotificationsServiceRolePolicy](#)
- [AWSCodeStarServiceRole](#)
- [AWSCompromisedKeyQuarantine](#)

- [AWSCompromisedKeyQuarantineV2](#)
- [AWSConfigMultiAccountSetupPolicy](#)
- [AWSConfigRemediationServiceRolePolicy](#)
- [AWSConfigRoleForOrganizations](#)
- [AWSConfigRulesExecutionRole](#)
- [AWSConfigServiceRolePolicy](#)
- [AWSConfigUserAccess](#)
- [AWSConnector](#)
- [AWSControlTowerAccountServiceRolePolicy](#)
- [AWSControlTowerServiceRolePolicy](#)
- [AWSCostAndUsageReportAutomationPolicy](#)
- [AWSDataExchangeFullAccess](#)
- [AWSDataExchangeProviderFullAccess](#)
- [AWSDataExchangeReadOnly](#)
- [AWSDataExchangeSubscriberFullAccess](#)
- [AWSDataLifecycleManagerServiceRole](#)
- [AWSDataLifecycleManagerServiceRoleForAMIManagement](#)
- [AWSDataLifecycleManagerSSMFullAccess](#)
- [AWSDataPipeline_FullAccess](#)
- [AWSDataPipeline_PowerUser](#)
- [AWSDataSyncDiscoveryServiceRolePolicy](#)
- [AWSDataSyncFullAccess](#)
- [AWSDataSyncReadOnlyAccess](#)
- [AWSDeadlineCloud-FleetWorker](#)
- [AWSDeadlineCloud-UserAccessFarms](#)
- [AWSDeadlineCloud-UserAccessFleets](#)
- [AWSDeadlineCloud-UserAccessJobs](#)
- [AWSDeadlineCloud-UserAccessQueues](#)
- [AWSDeadlineCloud-WorkerHost](#)

- [AWSDeepLensLambdaFunctionAccessPolicy](#)
- [AWSDeepLensServiceRolePolicy](#)
- [AWSDeepRacerAccountAdminAccess](#)
- [AWSDeepRacerCloudFormationAccessPolicy](#)
- [AWSDeepRacerDefaultMultiUserAccess](#)
- [AWSDeepRacerFullAccess](#)
- [AWSDeepRacerRoboMakerAccessPolicy](#)
- [AWSDeepRacerServiceRolePolicy](#)
- [AWSDenyAll](#)
- [AWSDeviceFarmFullAccess](#)
- [AWSDeviceFarmServiceRolePolicy](#)
- [AWSDeviceFarmTestGridServiceRolePolicy](#)
- [AWSDirectConnectFullAccess](#)
- [AWSDirectConnectReadOnlyAccess](#)
- [AWSDirectConnectServiceRolePolicy](#)
- [AWSDirectoryServiceFullAccess](#)
- [AWSDirectoryServiceReadOnlyAccess](#)
- [AWSDiscoveryContinuousExportFirehosePolicy](#)
- [AWSDMSFleetAdvisorServiceRolePolicy](#)
- [AWSDMSServerlessServiceRolePolicy](#)
- [AWSEC2CapacityReservationFleetRolePolicy](#)
- [AWSEC2FleetServiceRolePolicy](#)
- [AWSEC2SpotFleetServiceRolePolicy](#)
- [AWSEC2SpotServiceRolePolicy](#)
- [AWSEC2VssSnapshotPolicy](#)
- [AWSECRPullThroughCache_ServiceRolePolicy](#)
- [AWElasticBeanstalkCustomPlatformforEC2Role](#)
- [AWElasticBeanstalkEnhancedHealth](#)
- [AWElasticBeanstalkMaintenance](#)

- [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](#)
- [AWSIoTClickFullAccess](#)
- [AWSIoTClickReadOnlyAccess](#)
- [AWSIoTAnalyticsFullAccess](#)
- [AWSIoTAnalyticsReadOnlyAccess](#)
- [AWSIoTConfigAccess](#)
- [AWSIoTConfigReadOnlyAccess](#)
- [AWSIoTDataAccess](#)
- [AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction](#)
- [AWSIoTDeviceDefenderAudit](#)
- [AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction](#)
- [AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction](#)
- [AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateCACertMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction](#)
- [AWSIoTDeviceTesterForFreeRTOSFullAccess](#)
- [AWSIoTDeviceTesterForGreengrassFullAccess](#)
- [AWSIoTEventsFullAccess](#)
- [AWSIoTEventsReadOnlyAccess](#)
- [AWSIoTFleetHubFederationAccess](#)
- [AWSIoTFleetwiseServiceRolePolicy](#)
- [AWSIoTFullAccess](#)
- [AWSIoTLogging](#)
- [AWSIoTTOTALUpdate](#)
- [AWSIoTRoboRunnerFullAccess](#)

- [AWSIoTRoboRunnerReadOnly](#)
- [AWSIoTRoboRunnerServiceRolePolicy](#)
- [AWSIoTRuleActions](#)
- [AWSIoTSiteWiseConsoleFullAccess](#)
- [AWSIoTSiteWiseFullAccess](#)
- [AWSIoTSiteWiseMonitorPortalAccess](#)
- [AWSIoTSiteWiseMonitorServiceRolePolicy](#)
- [AWSIoTSiteWiseReadOnlyAccess](#)
- [AWSIoTThingsRegistration](#)
- [AWSIoTThingMakerServiceRolePolicy](#)
- [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](#)
- [AWSLambdaVPCLAccessExecutionRole](#)
- [AWSLicenseManagerConsumptionPolicy](#)
- [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)
- [AWSLicenseManagerMasterAccountRolePolicy](#)
- [AWSLicenseManagerMemberAccountRolePolicy](#)
- [AWSLicenseManagerServiceRolePolicy](#)
- [AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)
- [AWSM2ServicePolicy](#)
- [AWSManagedServices_ContactsServiceRolePolicy](#)
- [AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy](#)
- [AWSManagedServices_EventsServiceRolePolicy](#)
- [AWSManagedServicesDeploymentToolkitPolicy](#)
- [AWSMarketplaceAmiIngestion](#)
- [AWSMarketplaceDeploymentServiceRolePolicy](#)
- [AWSMarketplaceFullAccess](#)
- [AWSMarketplaceGetEntitlements](#)
- [AWSMarketplaceImageBuildFullAccess](#)
- [AWSMarketplaceLicenseManagementServiceRolePolicy](#)
- [AWSMarketplaceManageSubscriptions](#)
- [AWSMarketplaceMeteringFullAccess](#)
- [AWSMarketplaceMeteringRegisterUsage](#)
- [AWSMarketplaceProcurementSystemAdminFullAccess](#)

- [AWSMarketplacePurchaseOrdersServiceRolePolicy](#)
- [AWSMarketplaceRead-only](#)
- [AWSMarketplaceResaleAuthorizationServiceRolePolicy](#)
- [AWSMarketplaceSellerFullAccess](#)
- [AWSMarketplaceSellerProductsFullAccess](#)
- [AWSMarketplaceSellerProductsReadOnly](#)
- [AWSMediaConnectServicePolicy](#)
- [AWSMediaTailorServiceRolePolicy](#)
- [AWSMigrationHubDiscoveryAccess](#)
- [AWSMigrationHubDMSAccess](#)
- [AWSMigrationHubFullAccess](#)
- [AWSMigrationHubOrchestratorConsoleFullAccess](#)
- [AWSMigrationHubOrchestratorInstanceRolePolicy](#)
- [AWSMigrationHubOrchestratorPlugin](#)
- [AWSMigrationHubOrchestratorServiceRolePolicy](#)
- [AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess](#)
- [AWSMigrationHubRefactorSpaces-SSMAutomationPolicy](#)
- [AWSMigrationHubRefactorSpacesFullAccess](#)
- [AWSMigrationHubRefactorSpacesServiceRolePolicy](#)
- [AWSMigrationHubSMSAccess](#)
- [AWSMigrationHubStrategyCollector](#)
- [AWSMigrationHubStrategyConsoleFullAccess](#)
- [AWSMigrationHubStrategyServiceRolePolicy](#)
- [AWSMobileHub_FullAccess](#)
- [AWSMobileHub_ReadOnly](#)
- [AWSMSKReplicatorExecutionRole](#)
- [AWSNetworkFirewallServiceRolePolicy](#)
- [AWSNetworkManagerCloudWANServiceRolePolicy](#)
- [AWSNetworkManagerFullAccess](#)
- [AWSNetworkManagerReadOnlyAccess](#)

- [AWSNetworkManagerServiceRolePolicy](#)
- [AWSOpsWorks_FullAccess](#)
- [AWSOpsWorksCloudWatchLogs](#)
- [AWSOpsWorksCMInstanceProfileRole](#)
- [AWSOpsWorksCMServiceRole](#)
- [AWSOpsWorksInstanceRegistration](#)
- [AWSOpsWorksRegisterCLI_EC2](#)
- [AWSOpsWorksRegisterCLI_OnPremises](#)
- [AWSOrganizationsFullAccess](#)
- [AWSOrganizationsReadOnlyAccess](#)
- [AWSOrganizationsServiceTrustPolicy](#)
- [AWSOutpostsAuthorizeServerPolicy](#)
- [AWSOutpostsServiceRolePolicy](#)
- [AWSPanoramaApplianceRolePolicy](#)
- [AWSPanoramaApplianceServiceRolePolicy](#)
- [AWSPanoramaFullAccess](#)
- [AWSPanoramaGreengrassGroupRolePolicy](#)
- [AWSPanoramaSageMakerRolePolicy](#)
- [AWSPanoramaServiceLinkedRolePolicy](#)
- [AWSPanoramaServiceRolePolicy](#)
- [AWSPriceListServiceFullAccess](#)
- [AWSPrivateCAAuditor](#)
- [AWSPrivateCAFullAccess](#)
- [AWSPrivateCAPrivilegedUser](#)
- [AWSPrivateCARedOnly](#)
- [AWSPrivateCAUser](#)
- [AWSPrivateMarketplaceAdminFullAccess](#)
- [AWSPrivateMarketplaceRequests](#)
- [AWSPrivateNetworksServiceRolePolicy](#)
- [AWSProtonCodeBuildProvisioningBasicAccess](#)

- [AWSProtonCodeBuildProvisioningServiceRolePolicy](#)
- [AWSProtonDeveloperAccess](#)
- [AWSProtonFullAccess](#)
- [AWSProtonReadOnlyAccess](#)
- [AWSProtonServiceGitSyncServiceRolePolicy](#)
- [AWSProtonSyncServiceRolePolicy](#)
- [AWSPurchaseOrdersServiceRolePolicy](#)
- [AWSQuickSightAssetBundleExportPolicy](#)
- [AWSQuickSightAssetBundleImportPolicy](#)
- [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](#)
- [AWSServiceRoleForAmazonQDeveloper](#)
- [AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy](#)
- [AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy](#)
- [AWSServiceRoleForCodeGuru-Profiler](#)
- [AWSServiceRoleForCodeWhispererPolicy](#)

- [AWSServiceRoleForEC2ScheduledInstances](#)
- [AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy](#)
- [AWSServiceRoleForImageBuilder](#)
- [AWSServiceRoleForIoTSiteWise](#)
- [AWSServiceRoleForLogDeliveryPolicy](#)
- [AWSServiceRoleForMonitronPolicy](#)
- [AWSServiceRoleForNeptuneGraphPolicy](#)
- [AWSServiceRoleForPrivateMarketplaceAdminPolicy](#)
- [AWSServiceRoleForSMS](#)
- [AWSServiceRoleForUserSubscriptions](#)
- [AWSServiceRolePolicyForBackupReports](#)
- [AWSServiceRolePolicyForBackupRestoreTesting](#)
- [AWSShieldDRTAccessPolicy](#)
- [AWSShieldServiceRolePolicy](#)
- [AWSSSMForSAPServiceLinkedRolePolicy](#)
- [AWSSSMOpsInsightsServiceRolePolicy](#)
- [AWSSSODirectoryAdministrator](#)
- [AWSSSODirectoryReadOnly](#)
- [AWSSSOMasterAccountAdministrator](#)
- [AWSSSOMemberAccountAdministrator](#)
- [AWSSSORReadOnly](#)
- [AWSSSOServiceRolePolicy](#)
- [AWSStepFunctionsConsoleFullAccess](#)
- [AWSStepFunctionsFullAccess](#)
- [AWSStepFunctionsReadOnlyAccess](#)
- [AWSStorageGatewayFullAccess](#)
- [AWSStorageGatewayReadOnlyAccess](#)
- [AWSStorageGatewayServiceRolePolicy](#)
- [AWSSupplyChainFederationAdminAccess](#)
- [AWSsupportAccess](#)

- [AWSSupportAppFullAccess](#)
- [AWSSupportAppReadOnlyAccess](#)
- [AWSSupportPlansFullAccess](#)
- [AWSSupportPlansReadOnlyAccess](#)
- [AWSSupportServiceRolePolicy](#)
- [AWSSystemsManagerAccountDiscoveryServicePolicy](#)
- [AWSSystemsManagerChangeManagementServicePolicy](#)
- [AWSSystemsManagerForSAPFullAccess](#)
- [AWSSystemsManagerForSAPReadOnlyAccess](#)
- [AWSSystemsManagerOpsDataSyncServiceRolePolicy](#)
- [AWSThinkboxAssetServerPolicy](#)
- [AWSThinkboxAWSPortalAdminPolicy](#)
- [AWSThinkboxAWSPortalGatewayPolicy](#)
- [AWSThinkboxAWSPortalWorkerPolicy](#)
- [AWSThinkboxDeadlineResourceTrackerAccessPolicy](#)
- [AWSThinkboxDeadlineResourceTrackerAdminPolicy](#)
- [AWSThinkboxDeadlineSpotEventPluginAdminPolicy](#)
- [AWSThinkboxDeadlineSpotEventPluginWorkerPolicy](#)
- [AWSTransferConsoleFullAccess](#)
- [AWSTransferFullAccess](#)
- [AWSTransferLoggingAccess](#)
- [AWSTransferReadOnlyAccess](#)
- [AWSTrustedAdvisorPriorityFullAccess](#)
- [AWSTrustedAdvisorPriorityReadOnlyAccess](#)
- [AWSTrustedAdvisorReportingServiceRolePolicy](#)
- [AWSTrustedAdvisorServiceRolePolicy](#)
- [AWSUserNotificationsServiceLinkedRolePolicy](#)
- [AWSVendorInsightsAssessorFullAccess](#)
- [AWSVendorInsightsAssessorReadOnly](#)
- [AWSVendorInsightsVendorFullAccess](#)

- [AWSVendorInsightsVendorReadOnly](#)
- [AWSVpcLatticeServiceRolePolicy](#)
- [AWSVPCS2SVpnServiceRolePolicy](#)
- [AWSVPCTransitGatewayServiceRolePolicy](#)
- [AWSVPCVerifiedAccessServiceRolePolicy](#)
- [AWSWAFConsoleFullAccess](#)
- [AWSWAFConsoleReadOnlyAccess](#)
- [AWSWAFFullAccess](#)
- [AWSWAFReadOnlyAccess](#)
- [AWSWellArchitectedDiscoveryServiceRolePolicy](#)
- [AWSWellArchitectedOrganizationsServiceRolePolicy](#)
- [AWSWickrFullAccess](#)
- [AWSXrayCrossAccountSharingConfiguration](#)
- [AWSXRayDaemonWriteAccess](#)
- [AWSXrayFullAccess](#)
- [AWSXrayReadOnlyAccess](#)
- [AWSXrayWriteOnlyAccess](#)
- [AWSZonalAutoshiftPracticeRunSLRPolicy](#)
- [BatchServiceRolePolicy](#)
- [Billing](#)
- [CertificateManagerServiceRolePolicy](#)
- [ClientVPNServiceConnectionsRolePolicy](#)
- [ClientVPNServiceRolePolicy](#)
- [CloudFormationStackSetsOrgAdminServiceRolePolicy](#)
- [CloudFormationStackSetsOrgMemberServiceRolePolicy](#)
- [CloudFrontFullAccess](#)
- [CloudFrontReadOnlyAccess](#)
- [CloudHSMServiceRolePolicy](#)
- [CloudSearchFullAccess](#)
- [CloudSearchReadOnlyAccess](#)

- [CloudTrailServiceRolePolicy](#)
- [CloudWatch-CrossAccountAccess](#)
- [CloudWatchActionsEC2Access](#)
- [CloudWatchAgentAdminPolicy](#)
- [CloudWatchAgentServerPolicy](#)
- [CloudWatchApplicationInsightsFullAccess](#)
- [CloudWatchApplicationInsightsReadOnlyAccess](#)
- [CloudwatchApplicationInsightsServiceLinkedRolePolicy](#)
- [CloudWatchApplicationSignalsFullAccess](#)
- [CloudWatchApplicationSignalsReadOnlyAccess](#)
- [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](#)
- [EC2FastLaunchFullAccess](#)
- [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](#)
- [OpensearchIngestionSelfManagedVpcePolicy](#)
- [PartnerCentralAccountManagementUserRoleAssociation](#)
- [PowerUserAccess](#)
- [QBusinessServiceRolePolicy](#)
- [QuickSightAccessForS3StorageManagementAnalyticsReadOnly](#)
- [RDS CloudHsmAuthorizationRole](#)
- [ReadOnlyAccess](#)
- [ResourceGroupsandTagEditorFullAccess](#)
- [ResourceGroupsandTagEditorReadOnlyAccess](#)
- [ResourceGroupsServiceRolePolicy](#)
- [ROSAAmazonEBSCSIDriverOperatorPolicy](#)
- [ROSACloudNetworkConfigOperatorPolicy](#)

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

- [ViewOnlyAccess](#)
- [VMImportExportRoleForAWSConnector](#)
- [VPCLatticeFullAccess](#)
- [VPCLatticeReadOnlyAccess](#)
- [VPCLatticeServicesInvokeAccess](#)
- [WAFLoggingServiceRolePolicy](#)
- [WAFRegionalLoggingServiceRolePolicy](#)
- [WAFV2LoggingServiceRolePolicy](#)
- [WellArchitectedConsoleFullAccess](#)
- [WellArchitectedConsoleReadOnlyAccess](#)
- [WorkLinkServiceRolePolicy](#)

AccessAnalyzerServiceRolePolicy

Descrizione: consenti ad Access Analyzer di analizzare i metadati delle risorse

AccessAnalyzerServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 2 dicembre 2019, 17:13 UTC
- Ora modificata: 30 maggio 2024, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListUserPolicies",
        "iam:GetUserPolicy",

```



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

```
    "s3:GetMultiRegionAccessPointPolicyStatus",
    "s3:ListAccessPoints",
    "s3:ListAllMyBuckets",
    "s3:ListMultiRegionAccessPoints",
    "s3express:GetBucketPolicy",
    "s3express:ListAllMyDirectoryBuckets",
    "sns:GetTopicAttributes",
    "sns:ListTopics",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetResourcePolicy",
    "secretsmanager:ListSecrets",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AdministratorAccess

Descrizione: fornisce l'accesso completo a AWS servizi e risorse.

AdministratorAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AdministratorAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AdministratorAccess-Amplify

Descrizione: concede le autorizzazioni amministrative dell'account consentendo esplicitamente l'accesso diretto alle risorse necessarie alle applicazioni Amplify.

AdministratorAccess-Amplify [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AdministratorAccess-Amplify ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 19:03 UTC
- Ora modificata: 04 aprile 2024, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    "cloudformation:TagResource",
    "cloudformation:UntagResource"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/amplify-*"
  ]
},
{
  "Sid" : "CLIManageviaCFNPolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoleTags",
    "iam:TagRole",
    "iam:AttachRolePolicy",
    "iam:CreatePolicy",
    "iam:DeletePolicy",
    "iam:DeleteRole",
    "iam:DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePolicy",
    "iam:UntagRole",
    "iam:UpdateRole",
    "iam:GetRole",
    "iam:GetPolicy",
    "iam:GetRolePolicy",
    "iam:PassRole",
    "iam:ListPolicyVersions",
    "iam:CreatePolicyVersion",
    "iam:DeletePolicyVersion",
    "iam:CreateRole",
    "iam:ListRolePolicies",
    "iam:PutRolePermissionsBoundary",
    "iam:DeleteRolePermissionsBoundary",
    "appsync:CreateApiKey",
    "appsync:CreateDataSource",
    "appsync:CreateFunction",
    "appsync:CreateResolver",
    "appsync:CreateType",
    "appsync:DeleteApiKey",
    "appsync:DeleteDataSource",
    "appsync:DeleteFunction",
    "appsync:DeleteResolver",
    "appsync:DeleteType",
    "appsync:GetDataSource",
```

```
"appsync:GetFunction",
"appsync:GetIntrospectionSchema",
"appsync:GetResolver",
"appsync:GetSchemaCreationStatus",
"appsync:GetType",
"appsync:GraphQL",
"appsync:ListApiKeys",
"appsync:ListDataSources",
"appsync:ListFunctions",
"appsync:ListGraphqlApis",
"appsync:ListResolvers",
"appsync:ListResolversByFunction",
"appsync:ListTypes",
"appsync:StartSchemaCreation",
"appsync:UntagResource",
"appsync:UpdateApiKey",
"appsync:UpdateDataSource",
"appsync:UpdateFunction",
"appsync:UpdateResolver",
"appsync:UpdateType",
"appsync:TagResource",
"appsync:CreateGraphqlApi",
"appsync>DeleteGraphqlApi",
"appsync:GetGraphqlApi",
"appsync:ListTagsForResource",
"appsync:UpdateGraphqlApi",
"apigateway:DELETE",
"apigateway:GET",
"apigateway:PATCH",
"apigateway:POST",
"apigateway:PUT",
"cognito-idp:CreateUserPool",
"cognito-identity:CreateIdentityPool",
"cognito-identity>DeleteIdentityPool",
"cognito-identity:DescribeIdentity",
"cognito-identity:DescribeIdentityPool",
"cognito-identity:SetIdentityPoolRoles",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:UpdateIdentityPool",
"cognito-idp:CreateUserPoolClient",
"cognito-idp>DeleteUserPool",
"cognito-idp>DeleteUserPoolClient",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
```

```
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserPoolClients",
"cognito-idp:UpdateUserPoolClient",
"cognito-idp:CreateGroup",
"cognito-idp:DeleteGroup",
"cognito-identity:TagResource",
"cognito-idp:TagResource",
"cognito-idp:UpdateUserPool",
"cognito-idp:SetUserPoolMfaConfig",
"lambda:AddPermission",
"lambda:CreateFunction",
"lambda:DeleteFunction",
"lambda:GetFunction",
"lambda:GetFunctionConfiguration",
"lambda:InvokeAsync",
"lambda:InvokeFunction",
"lambda:RemovePermission",
"lambda:UpdateFunctionCode",
"lambda:UpdateFunctionConfiguration",
"lambda:ListTags",
"lambda:TagResource",
"lambda:UntagResource",
"lambda:AddLayerVersionPermission",
"lambda:CreateEventSourceMapping",
"lambda:DeleteEventSourceMapping",
"lambda:DeleteLayerVersion",
"lambda:GetEventSourceMapping",
"lambda:GetLayerVersion",
"lambda:ListEventSourceMappings",
"lambda:ListLayerVersions",
"lambda:PublishLayerVersion",
"lambda:RemoveLayerVersionPermission",
"lambda:UpdateEventSourceMapping",
"dynamodb:CreateTable",
"dynamodb:DeleteItem",
"dynamodb:DeleteTable",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListStreams",
"dynamodb:PutItem",
"dynamodb:TagResource",
"dynamodb:ListTagsOfResource",
"dynamodb:UntagResource",
```

```
"dynamodb:UpdateContinuousBackups",
"dynamodb:UpdateItem",
"dynamodb:UpdateTable",
"dynamodb:UpdateTimeToLive",
"s3:CreateBucket",
"s3:ListBucket",
"s3:PutBucketAcl",
"s3:PutBucketCORS",
"s3:PutBucketNotification",
"s3:PutBucketPolicy",
"s3:PutBucketWebsite",
"s3:PutObjectAcl",
"cloudfront:CreateCloudFrontOriginAccessIdentity",
"cloudfront:CreateDistribution",
"cloudfront>DeleteCloudFrontOriginAccessIdentity",
"cloudfront>DeleteDistribution",
"cloudfront:GetCloudFrontOriginAccessIdentity",
"cloudfront:GetCloudFrontOriginAccessIdentityConfig",
"cloudfront:GetDistribution",
"cloudfront:GetDistributionConfig",
"cloudfront:TagResource",
"cloudfront:UntagResource",
"cloudfront:UpdateCloudFrontOriginAccessIdentity",
"cloudfront:UpdateDistribution",
"events:DeleteRule",
"events:DescribeRule",
"events:ListRuleNamesByTarget",
"events:PutRule",
"events:PutTargets",
"events:RemoveTargets",
"mobiletargeting:GetApp",
"kinesis:AddTagsToStream",
"kinesis:CreateStream",
"kinesis>DeleteStream",
"kinesis:DescribeStream",
"kinesis:DescribeStreamSummary",
"kinesis:ListTagsForStream",
"kinesis:PutRecords",
"es:AddTags",
"es:CreateElasticsearchDomain",
"es>DeleteElasticsearchDomain",
"es:DescribeElasticsearchDomain",
"es:UpdateElasticsearchDomainConfig",
"s3:PutEncryptionConfiguration",
```



```

    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "CLISDKCalls",
  "Effect" : "Allow",
  "Action" : [
    "appsync:GetIntrospectionSchema",
    "appsync:GraphQL",
    "appsync:UpdateApiKey",
    "appsync:ListApiKeys",
    "amplify:*",
    "amplifybackend:*",
    "amplifyuibuilder:*",
    "sts:AssumeRole",
    "mobiletargeting:*",
    "cognito-idp:AdminAddUserToGroup",
    "cognito-idp:AdminCreateUser",
    "cognito-idp:CreateGroup",
    "cognito-idp>DeleteGroup",
    "cognito-idp>DeleteUser",
    "cognito-idp:ListUsers",
    "cognito-idp:AdminGetUser",
    "cognito-idp:ListUsersInGroup",
    "cognito-idp:AdminDisableUser",
    "cognito-idp:AdminRemoveUserFromGroup",
    "cognito-idp:AdminResetUserPassword",
    "cognito-idp:AdminListGroupsForUser",
    "cognito-idp:ListGroups",
    "cognito-idp:AdminListUserAuthEvents",
    "cognito-idp:AdminDeleteUser",
    "cognito-idp:AdminConfirmSignUp",
    "cognito-idp:AdminEnableUser",
    "cognito-idp:AdminUpdateUserAttributes",
    "cognito-idp:DescribeIdentityProvider",
    "cognito-idp:DescribeUserPool",

```

```
"cognito-idp:DeleteUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:CreateUserPool",
"cognito-idp:CreateUserPoolClient",
"cognito-idp:UpdateUserPool",
"cognito-idp:AdminSetUserPassword",
"cognito-idp:ListUserPools",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListIdentityProviders",
"cognito-idp:GetUserPoolMfaConfig",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:SetIdentityPoolRoles",
"cognito-identity:CreateIdentityPool",
"cognito-identity:DeleteIdentityPool",
"cognito-identity:ListIdentityPools",
"cognito-identity:DescribeIdentityPool",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"lambda:GetFunction",
"lambda:CreateFunction",
"lambda:AddPermission",
"lambda:DeleteFunction",
"lambda:DeleteLayerVersion",
"lambda:InvokeFunction",
"lambda:ListLayerVersions",
"iam:PutRolePolicy",
"iam:CreatePolicy",
"iam:AttachRolePolicy",
"iam:ListPolicyVersions",
"iam:ListAttachedRolePolicies",
"iam:CreateRole",
"iam:PassRole",
"iam:ListRolePolicies",
"iam:DeleteRolePolicy",
"iam:CreatePolicyVersion",
"iam:DeletePolicyVersion",
"iam:DeleteRole",
"iam:DetachRolePolicy",
"cloudformation:ListStacks",
"cloudformation:DescribeStacks",
"sns:CreateSMSSandboxPhoneNumber",
"sns:GetSMSSandboxAccountStatus",
"sns:VerifySMSSandboxPhoneNumber",
"sns:DeleteSMSSandboxPhoneNumber",
```

```

        "sns:ListSMSSandboxPhoneNumbers",
        "sns:ListOriginationNumbers",
        "rekognition:DescribeCollection",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "lex:GetBot",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "cloudformation:GetTemplateSummary",
        "codecommit:GitPull",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "polly:DescribeVoices"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AmplifySSMCalls",
    "Effect" : "Allow",
    "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "ssm:DeleteParameters"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*"
},
{
    "Sid" : "GeoPowerUser",
    "Effect" : "Allow",
    "Action" : [
        "geo:*"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AmplifyEcrSDKCalls",
    "Effect" : "Allow",
    "Action" : [
        "ecr:DescribeRepositories"
    ],

```

```
    "Resource" : "*"
  },
  {
    "Sid" : "AmplifyStorageSDKCalls",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:DeleteBucket",
      "s3:DeleteBucketPolicy",
      "s3:DeleteBucketWebsite",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:ListBucketVersions",
      "s3:PutBucketAcl",
      "s3:PutBucketCORS",
      "s3:PutBucketNotification",
      "s3:PutBucketPolicy",
      "s3:PutBucketVersioning",
      "s3:PutBucketWebsite",
      "s3:PutEncryptionConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmplifySSRCalls",
    "Effect" : "Allow",
    "Action" : [
      "cloudfront:CreateCloudFrontOriginAccessIdentity",
      "cloudfront:CreateDistribution",
      "cloudfront:CreateInvalidation",
      "cloudfront:GetDistribution",
      "cloudfront:GetDistributionConfig",
      "cloudfront:ListCloudFrontOriginAccessIdentities",
      "cloudfront:ListDistributions",
      "cloudfront:ListDistributionsByLambdaFunction",
      "cloudfront:ListDistributionsByWebACLId",
      "cloudfront:ListFieldLevelEncryptionConfigs",
```

```
"cloudfront:ListFieldLevelEncryptionProfiles",
"cloudfront:ListInvalidations",
"cloudfront:ListPublicKeys",
"cloudfront:ListStreamingDistributions",
"cloudfront:UpdateDistribution",
"cloudfront:TagResource",
"cloudfront:UntagResource",
"cloudfront:ListTagsForResource",
"cloudfront:DeleteDistribution",
"iam:AttachRolePolicy",
"iam:CreateRole",
"iam:CreateServiceLinkedRole",
"iam:GetRole",
"iam:PutRolePolicy",
"iam:PassRole",
"lambda:CreateFunction",
"lambda:EnableReplication",
"lambda:DeleteFunction",
"lambda:GetFunction",
"lambda:GetFunctionConfiguration",
"lambda:PublishVersion",
"lambda:UpdateFunctionCode",
"lambda:UpdateFunctionConfiguration",
"lambda:ListTags",
"lambda:TagResource",
"lambda:UntagResource",
"route53:ChangeResourceRecordSets",
"route53:ListHostedZonesByName",
"route53:ListResourceRecordSets",
"s3:CreateBucket",
"s3:GetAccelerateConfiguration",
"s3:GetObject",
"s3:ListBucket",
"s3:PutAccelerateConfiguration",
"s3:PutBucketPolicy",
"s3:PutObject",
"s3:PutBucketTagging",
"s3:GetBucketTagging",
"lambda:ListEventSourceMappings",
"lambda:CreateEventSourceMapping",
"iam:UpdateAssumeRolePolicy",
"iam:DeleteRolePolicy",
"sqs:CreateQueue",
"sqs:DeleteQueue",
```

```

        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:UpdateApp",
        "amplify:UpdateBranch"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AmplifySSRViewLogGroups",
    "Effect" : "Allow",
    "Action" : "logs:DescribeLogGroups",
    "Resource" : "arn:aws:logs:*:*:log-group:*"
},
{
    "Sid" : "AmplifySSRCreateLogGroup",
    "Effect" : "Allow",
    "Action" : "logs:CreateLogGroup",
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*"
},
{
    "Sid" : "AmplifySSRPushLogs",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*:log-stream:*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AdministratorAccess-AWSElasticBeanstalk

Descrizione: concede le autorizzazioni amministrative dell'account. Consente esplicitamente a sviluppatori e amministratori di accedere direttamente alle risorse necessarie per gestire le applicazioni Elastic AWS Beanstalk

AdministratorAccess-AWSElasticBeanstalk [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AdministratorAccess-AWSElasticBeanstalk ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 gennaio 2021, 19:36 UTC
- Ora modificata: 23 marzo 2023, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AlexaForBusinessDeviceSetup

Descrizione: Fornisci l'accesso ai AlexaForBusiness servizi per la configurazione del dispositivo

AlexaForBusinessDeviceSetup è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AlexaForBusinessDeviceSetup ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:47 UTC
- Ora modificata: 20 maggio 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AlexaForBusinessFullAccess

Descrizione: garantisce l'accesso completo alle AlexaForBusiness risorse e l'accesso alle risorse correlate Servizi AWS

AlexaForBusinessFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AlexaForBusinessFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:47 UTC

- Ora modificata: 01 luglio 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AlexaForBusinessGatewayExecution

Descrizione: Fornisci l'accesso di esecuzione del gateway ai AlexaForBusiness servizi

AlexaForBusinessGatewayExecution è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AlexaForBusinessGatewayExecution` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:47 UTC
- Ora modificata: 30 novembre 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

Descrizione: Fornisci l'accesso ai dispositivi Lifesize AVS

AlexaForBusinessLifesizeDelegatedAccessPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AlexaForBusinessLifesizeDelegatedAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 giugno 2020, 19:46 UTC

- Ora modificata: 12 giugno 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*/*:A2IW07UEGW4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IW07UEGW4TL"
          ]
        }
      }
    }
  ]
}
```

```

    ]
  }
}
},
{
  "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/*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AlexaForBusinessNetworkProfileServicePolicy

Descrizione: questa politica consente ad Alexa for Business di eseguire attività automatizzate pianificate dai tuoi profili di rete.

AlexaForBusinessNetworkProfileServicePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 marzo 2019, 00:53 UTC
- Ora modificata: 5 aprile 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AlexaForBusinessPolyDelegatedAccessPolicy

Descrizione: Fornisci l'accesso ai dispositivi Poly AVS

AlexaForBusinessPolyDelegatedAccessPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AlexaForBusinessPolyDelegatedAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 16 ottobre 2019, 19:48 UTC
- Ora modificata: 16 ottobre 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b>DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A238TWV36W3S92",
            "A1FUZ1SC53VJXD"
          ]
        }
      }
    },
    {
      "Action" : [
        "a4b:SearchDevices"
      ],
```

```

    "Effect" : "Allow",
    "Resource" : [
        "*"
    ]
},
{
    "Action" : [
        "a4b:AssociateDeviceWithRoom"
    ],
    "Effect" : "Allow",
    "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD",
        "arn:aws:a4b:us-east-1:*:room/*"
    ]
},
{
    "Action" : [
        "a4b:GetRoom",
        "a4b:SearchRooms",
        "a4b:CreateRoom",
        "a4b:GetProfile",
        "a4b:SearchSkillGroups",
        "a4b:DisassociateSkillGroupFromRoom",
        "a4b:AssociateSkillGroupWithRoom",
        "a4b:GetSkillGroup",
        "a4b:SearchProfiles",
        "a4b:GetAddressBook",
        "a4b:UpdateRoom"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AlexaForBusinessReadOnlyAccess

Descrizione: Fornisci l'accesso in sola lettura ai AlexaForBusiness servizi

AlexaForBusinessReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AlexaForBusinessReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:47 UTC
- Ora modificata: 20 novembre 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAPIGatewayAdministrator

Descrizione: fornisce l'accesso completo per creare/modificare/eliminare le API in Amazon API Gateway tramite AWS Management Console

AmazonAPIGatewayAdministrator [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonAPIGatewayAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:34 UTC
- Ora modificata: 9 luglio 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAPIGatewayInvokeFullAccess

Descrizione: fornisce l'accesso completo alle API di richiamo in Amazon API Gateway.

AmazonAPIGatewayInvokeFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonAPIGatewayInvokeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:36 UTC
- Ora modificata: 18 dicembre 2018, 18:25 UTC

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

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAPIGatewayPushToCloudWatchLogs

Descrizione: consente ad API Gateway di inviare i log all'account dell'utente.

AmazonAPIGatewayPushToCloudWatchLogs è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonAPIGatewayPushToCloudWatchLogs ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 novembre 2015, 23:41 UTC
- Ora modificata: 11 novembre 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAppFlowFullAccess

Descrizione: fornisce l'accesso completo ad Amazon AppFlow e l'accesso ai AWS servizi supportati come origine o destinazione del flusso (S3 e Redshift). Fornisce inoltre l'accesso a KMS per la crittografia

AmazonAppFlowFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonAppFlowFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 giugno 2020, 23:30 UTC
- Ora modificata: 28 febbraio 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAppFlowReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ai flussi di Amazon Appflow

AmazonAppFlowReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonAppFlowReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 giugno 2020, 23:26 UTC
- Ora modificata: 28 febbraio 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAppStreamFullAccess

Descrizione: fornisce l'accesso completo ad Amazon AppStream tramite AWS Management Console.

AmazonAppStreamFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonAppStreamFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 28 agosto 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAppStreamPCAAccess

Descrizione: accesso Amazon AppStream 2.0 alla CA privata di AWS Certificate Manager negli account dei clienti per l'autenticazione basata su certificati

AmazonAppStreamPCAAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonAppStreamPCAAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 ottobre 2022, 17:05 UTC
- Ora modificata: 24 ottobre 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAppStreamReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon AppStream tramite AWS Management Console.

AmazonAppStreamReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonAppStreamReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 7 dicembre 2016, 21:00 UTC

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

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAppStreamServiceAccess

Descrizione: politica predefinita per il ruolo AppStream di servizio Amazon.

AmazonAppStreamServiceAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonAppStreamServiceAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 novembre 2016, 04:17 UTC
- Ora modificata: 26 giugno 2020, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAthenaFullAccess

Descrizione: Fornisci accesso completo ad Amazon Athena e accesso mirato alle dipendenze necessarie per consentire l'esecuzione di query, la scrittura dei risultati e la gestione dei dati.

AmazonAthenaFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonAthenaFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 16:46 UTC
- Ora modificata: 03 gennaio 2024, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAugmentedAIFullAccess

Descrizione: fornisce l'accesso per eseguire tutte le operazioni, le risorse Amazon Augmented AI HumanTaskUis , FlowDefinitions HumanLoops tra cui e. Non consente l'accesso per creare FlowDefinitions contro il pubblico Workteam.

AmazonAugmentedAIFullAccess [è una politica gestita AWS](#) .

Utilizzo di questa politica

Puoi collegarti AmazonAugmentedAIFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 16:21 UTC
- Ora modificata: 03 dicembre 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
                ]
            }
        }
    }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAugmentedAIHumanLoopFullAccess

Descrizione: fornisce l'accesso per eseguire tutte le operazioni su HumanLoops.

AmazonAugmentedAIHumanLoopFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonAugmentedAIHumanLoopFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 16:20 UTC
- Ora modificata: 03 dicembre 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonAugmentedAIIntegratedAPIAccess

Descrizione: fornisce l'accesso per eseguire tutte le operazioni, le risorse Amazon Augmented AI HumanTaskUis , FlowDefinitions HumanLoops tra cui e. Fornisce inoltre l'accesso a quelle operazioni dei servizi integrati con Amazon Augmented AI.

AmazonAugmentedAIIntegratedAPIAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonAugmentedAIIntegratedAPIAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 aprile 2020, 20:47 UTC
- Ora modificata: 22 aprile 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "textextract: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"
        ]
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonBedrockFullAccess

Descrizione: Fornisce accesso completo ad Amazon Bedrock e accesso limitato ai servizi correlati da esso richiesti

AmazonBedrockFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonBedrockFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 dicembre 2023, 15:47 UTC
- Ora modificata: 06 dicembre 2023, 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonBedrockReadOnly

Descrizione: Fornisce accesso in sola lettura ad Amazon Bedrock

AmazonBedrockReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonBedrockReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 dicembre 2023, 15:48 UTC
- Ora modificata: 06 dicembre 2023, 15:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonBraketFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Braket tramite l'SDK AWS Management Console and. Fornisce inoltre l'accesso ai servizi correlati (ad esempio, S3, log).

AmazonBraketFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonBraketFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 agosto 2020, 20:12 UTC
- Ora modificata: 19 aprile 2023, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonBraketJobsExecutionPolicy

Descrizione: concede l'accesso Servizi AWS e le risorse necessarie per l'esecuzione di un Amazon Braket Job tra cui S3, Cloudwatch, IAM e Braket

AmazonBraketJobsExecutionPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonBraketJobsExecutionPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 novembre 2021, 19:34 UTC
- Ora modificata: 28 novembre 2021, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}

```

```
}  
  }  
    }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonBraketServiceRolePolicy

Descrizione: Consente ad Amazon Braket di creare e gestire AWS risorse per tuo conto

AmazonBraketServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 4 agosto 2020, 17:12 UTC
- Ora modificata: 6 agosto 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeFullAccess

Descrizione: fornisce l'accesso completo alla Console di amministrazione di Amazon Chime tramite AWS Management Console

AmazonChimeFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonChimeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 novembre 2017, 22:15 UTC
- Ora modificata: 14 dicembre 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeReadOnly

Descrizione: fornisce l'accesso in sola lettura alla Console di amministrazione di Amazon Chime tramite. AWS Management Console

AmazonChimeReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonChimeReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 novembre 2017, 22:04 UTC
- Ora modificata: 14 dicembre 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeSDK

Descrizione: Fornisce l'accesso alle operazioni dell'SDK Amazon Chime

AmazonChimeSDK è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonChimeSDK ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 febbraio 2020, 21:53 UTC
- Ora modificata: 10 gennaio 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Descrizione: Policy gestita per il ruolo collegato al servizio Amazon Chime SDK MediaPipelines

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 4 aprile 2022, 22:02 UTC
- Ora modificata: 08 dicembre 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"br/>  }  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeSDKMessagingServiceRolePolicy

Descrizione: consente ad Amazon Chime SDK Messaging di accedere alle AWS risorse e abilitare la funzionalità di messaggistica

AmazonChimeSDKMessagingServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 03 marzo 2023, 01:43 UTC
- Ora modificata: 03 marzo 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeServiceRolePolicy

Descrizione: consente l'accesso alle AWS risorse utilizzate o gestite da Amazon Chime

AmazonChimeServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 settembre 2019, 22:25 UTC
- Ora modificata: 30 settembre 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```



```
}  
  }  
    }  
  ]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

Descrizione: consente ad Amazon Chime di accedere ad Amazon Transcribe e Amazon Transcribe Medical per tuo conto

AmazonChimeTranscriptionServiceLinkedRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 4 agosto 2021, 21:47 UTC
- Ora modificata: 04 agosto 2021, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeUserManagement

Descrizione: fornisce l'accesso alla gestione degli utenti alla Console di amministrazione di Amazon Chime tramite AWS Management Console

AmazonChimeUserManagement è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonChimeUserManagement ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 novembre 2017, 22:17 UTC
- Ora modificata: 18 febbraio 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroups",
        "chime:SubmitSupportRequest",
        "chime:ListDelegates",
        "chime:ListAccountUsageReportData",
        "chime:GetMeetingDetail",
        "chime:ListMeetingEvents",
        "chime:ListMeetingsReportData",
        "chime:GetUserActivityReportData",
        "chime:UpdateUser",
        "chime:BatchUpdateUser",
        "chime:BatchSuspendUser",
```

```
    "chime:BatchUnsuspendUser",
    "chime:AssociatePhoneNumberWithUser",
    "chime:DisassociatePhoneNumberFromUser",
    "chime:GetPhoneNumber",
    "chime:ListPhoneNumbers",
    "chime:GetUserSettings",
    "chime:UpdateUserSettings",
    "chime:CreateUser",
    "chime:AssociateSigninDelegateGroupsWithAccount",
    "chime:DisassociateSigninDelegateGroupsFromAccount"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Descrizione: policy gestita per Service Linked Role per Amazon Chime VoiceConnector

AmazonChimeVoiceConnectorServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 settembre 2019, 22:16 UTC

- Ora modificata: 14 aprile 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
      "*"
    ]
  }
}
```

```
]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCloudDirectoryFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Cloud Directory Service.

AmazonCloudDirectoryFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCloudDirectoryFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 febbraio 2017, 00:41 UTC
- Ora modificata: 25 febbraio 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCloudDirectoryReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Cloud Directory Service.

AmazonCloudDirectoryReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCloudDirectoryReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 febbraio 2017, 23:42 UTC
- Ora modificata: 28 febbraio 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCloudWatchEvidentlyFullAccess

Descrizione: fornisce solo l'accesso completo ad Amazon CloudWatch Evidently. Fornisce inoltre l'accesso ad Amazon S3, Amazon SNS, CloudWatch Amazon e altri servizi correlati.

AmazonCloudWatchEvidentlyFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCloudWatchEvidentlyFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 15:10 UTC
- Ora modificata: 29 novembre 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon CloudWatch Evidently

AmazonCloudWatchEvidentlyReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCloudWatchEvidentlyReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 15:08 UTC
- Ora modificata: 29 novembre 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

Descrizione: consente a CloudWatch Evidently Service di gestire AWS le risorse associate per conto del cliente

AmazonCloudWatchEvidentlyServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 settembre 2022, 17:25 UTC

- Ora modificata: 13 settembre 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCloudWatchRUMFullAccess

Descrizione: concede le autorizzazioni di accesso complete per il servizio Amazon RUM CloudWatch

AmazonCloudWatchRUMFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonCloudWatchRUMFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 15:46 UTC
- Ora modificata: 29 novembre 2021, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCloudWatchRUMReadOnlyAccess

Descrizione: concede autorizzazioni di sola lettura per il servizio Amazon RUM CloudWatch

AmazonCloudWatchRUMReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCloudWatchRUMReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 15:43 UTC
- Ora modificata: 28 ottobre 2022, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCloudWatchRUMServiceRolePolicy

Descrizione: concede l'autorizzazione ad Amazon CloudWatch RUM Service per pubblicare dati di monitoraggio su altri servizi pertinenti AWS

AmazonCloudWatchRUMServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 novembre 2021, 23:17 UTC

- Ora modificata: 22 febbraio 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeCatalystFullAccess

Descrizione: Fornisce accesso completo ad Amazon CodeCatalyst

AmazonCodeCatalystFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeCatalystFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2023, 16:50 UTC
- Ora modificata: 20 aprile 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeCatalystReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon CodeCatalyst

AmazonCodeCatalystReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeCatalystReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2023, 16:49 UTC
- Ora modificata: 20 aprile 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeCatalystSupportAccess

Descrizione: consente CodeCatalyst ad Amazon di creare, aggiornare e risolvere i AWS Support casi per tuo conto.

AmazonCodeCatalystSupportAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeCatalystSupportAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 12:34 UTC
- Ora modificata: 20 aprile 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeGuruProfilerAgentAccess

Descrizione: fornisce l'accesso richiesto dall'agente Amazon CodeGuru Profiler.

AmazonCodeGuruProfilerAgentAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeGuruProfilerAgentAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 febbraio 2021, 22:11 UTC
- Ora modificata: 5 maggio 2022, 18:11 UTC

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

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeGuruProfilerFullAccess

Descrizione: fornisce l'accesso completo ad Amazon CodeGuru Profiler.

AmazonCodeGuruProfilerFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeGuruProfilerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 10:13 UTC
- Ora modificata: 15 luglio 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeGuruProfilerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon CodeGuru Profiler.

AmazonCodeGuruProfilerReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeGuruProfilerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 3 dicembre 2019, 10:30 UTC
- Ora modificata: 27 giugno 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeGuruReviewerFullAccess

Descrizione: concede l'accesso completo ad Amazon CodeGuru Reviewer e l'accesso mirato alle dipendenze richieste.

AmazonCodeGuruReviewerFullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AmazonCodeGuruReviewerFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 08:33 UTC
- Ora modificata: 29 agosto 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeGuruReviewerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon CodeGuru Reviewer.

AmazonCodeGuruReviewerReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeGuruReviewerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 08:48 UTC
- Ora modificata: 29 agosto 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeGuruReviewerServiceRolePolicy

Descrizione: un ruolo collegato al servizio richiesto ad Amazon CodeGuru Reviewer per accedere alle risorse per tuo conto.

AmazonCodeGuruReviewerServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 03 dicembre 2019, 05:31 UTC

- Ora modificata: 27 novembre 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*/*"
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeGuruSecurityFullAccess

Descrizione: fornisce l'accesso completo ad Amazon CodeGuru Security.

AmazonCodeGuruSecurityFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeGuruSecurityFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2023, 21:03 UTC
- Ora modificata: 09 maggio 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCodeGuruSecurityScanAccess

Descrizione: fornisce l'accesso necessario per lavorare con le scansioni CodeGuru di Amazon Security.

AmazonCodeGuruSecurityScanAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCodeGuruSecurityScanAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2023, 20:54 UTC
- Ora modificata: 09 maggio 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCognitoDeveloperAuthenticatedIdentities

Descrizione: fornisce l'accesso alle API di Amazon Cognito per supportare le identità autenticate degli sviluppatori dal tuo backend di autenticazione.

AmazonCognitoDeveloperAuthenticatedIdentities [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonCognitoDeveloperAuthenticatedIdentities ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 marzo 2015, 17:22 UTC
- Ora modificata: 24 marzo 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Effect" : "Allow",
"Action" : [
  "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
  "cognito-identity:LookupDeveloperIdentity",
  "cognito-identity:MergeDeveloperIdentities",
  "cognito-identity:UnlinkDeveloperIdentity"
],
"Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCognitoIdpEmailServiceRolePolicy

Descrizione: consente al servizio Amazon Cognito User Pools di utilizzare le identità SES per l'invio di e-mail

AmazonCognitoIdpEmailServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 marzo 2019, 21:32 UTC
- Ora modificata: 21 marzo 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCognitoIdpServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite dai pool di utenti di Amazon Cognito

AmazonCognitoIdpServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 giugno 2020, 22:30 UTC
- Ora modificata: 26 giugno 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCognitoPowerUser

Descrizione: fornisce l'accesso amministrativo alle risorse Amazon Cognito esistenti. Avrai bisogno dei privilegi di Account AWS amministratore per creare nuove risorse Cognito.

AmazonCognitoPowerUser è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCognitoPowerUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 marzo 2015, 17:14 UTC
- Ora modificata: 01 giugno 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCognitoReadOnly

Descrizione: fornisce accesso in sola lettura alle risorse di Amazon Cognito.

AmazonCognitoReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonCognitoReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 marzo 2015, 17:06 UTC
- Ora modificata: 01 agosto 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Descrizione: questa politica definisce l'insieme di autorizzazioni consentite per le identità non autenticate per i pool di identità di Cognito. Questa politica non è pensata per essere utilizzata come

politica di autorizzazione autonoma. Viene utilizzata come barriera contro le politiche eccessivamente permissive relative ai ruoli in un pool di identità. Non associate questa policy a nessun ruolo, poiché Cognito Identity Service la includerà automaticamente come policy ristretta al momento della creazione delle credenziali. I privilegi per accedere temporaneamente ad altre AWS risorse tramite il flusso avanzato saranno ora definiti dall'intersezione tra il ruolo associato all'identità dell'utente non autenticato fornito da un servizio e i privilegi concessi in questa politica gestita di proprietà di Cognito.

AmazonCognitoUnAuthedIdentitiesSessionPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonCognitoUnAuthedIdentitiesSessionPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 luglio 2023, 23:04 UTC
- Ora modificata: 19 luglio 2023, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
```

```
    "polly:*",
    "comprehend:*",
    "translate:*",
    "transcribe:*",
    "rekognition:*",
    "mobiletargeting:*",
    "firehose:*",
    "personalize:*"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonCognitoUnauthenticatedIdentities

Descrizione: questa politica definisce l'insieme di autorizzazioni consentite per le identità non autenticate per i pool di identità di Cognito. Non è necessario che questo sia associato al ruolo unauth, poiché Cognito Identity Service lo includerà automaticamente come policy ristretta durante la creazione delle credenziali. I privilegi per accedere temporaneamente ad altre AWS risorse tramite il flusso avanzato saranno ora definiti dall'intersezione tra il ruolo associato all'identità dell'utente non autenticato fornito da un servizio e i privilegi concessi in questa politica gestita di proprietà di Cognito.

AmazonCognitoUnauthenticatedIdentities [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonCognitoUnauthenticatedIdentities ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 1 febbraio 2023, 22:36 UTC
- Ora modificata: 01 febbraio 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonConnect_FullAccess

Descrizione: lo scopo di questa politica è concedere le autorizzazioni agli utenti AWS Connect necessari per utilizzare le risorse Connect. Questa policy fornisce l'accesso completo alle risorse AWS Connect tramite Connect Console e API pubbliche.

AmazonConnect_FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonConnect_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2020, 19:54 UTC
- Ora modificata: 07 marzo 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}

```

```
}  
  }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

Descrizione: Policy per il ruolo collegato al servizio Amazon Connect Campaigns

AmazonConnectCampaignsServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 settembre 2021, 20:54 UTC
- Ora modificata: 08 novembre 2023, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonConnectReadOnlyAccess

Descrizione: concede l'autorizzazione a visualizzare le istanze Amazon Connect nel tuo Account AWS

AmazonConnectReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonConnectReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 ottobre 2018, 21:00 UTC
- Ora modificata: 6 novembre 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonConnectServiceLinkedRolePolicy

Descrizione: consente ad Amazon Connect di creare e gestire AWS risorse per tuo conto.

AmazonConnectServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 07 settembre 2018, 00:21 UTC
- Ora modificata: 24 maggio 2024, 01:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v16 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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",
        "wisdom:ListContentAssociations"
    ],
    "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}"
    }
  }
},
{
  "Sid" : "AllowCognitoForConnectEnabledTaggedResources",
  "Effect" : "Allow",
  "Action" : [
    "cognito-idp:DescribeUserPool",
    "cognito-idp:ListUserPoolClients"
  ],
  "Resource" : "arn:aws:cognito-idp:*:*:userpool/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonConnectEnabled" : "True"
    }
  }
},
{
  "Sid" : "AllowWritePermissionForCustomerProfileObjects",
  "Effect" : "Allow",
  "Action" : [
    "profile:PutProfileObject"
```



```
    ],  
    "Resource" : [  
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"  
    ]  
  }  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonConnectSynchronizationServiceRolePolicy

Descrizione: consente ad Amazon Connect di sincronizzare AWS le risorse tra le regioni per tuo conto.

AmazonConnectSynchronizationServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 27 ottobre 2023, 22:38 UTC
- Ora modificata: 27 ottobre 2023, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
}

```

```
]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonConnectVoiceIDFullAccess

Descrizione: Fornisce accesso completo a Amazon Connect Voice ID

AmazonConnectVoiceIDFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonConnectVoiceIDFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 settembre 2021, 19:04 UTC
- Ora modificata: 26 settembre 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneDomainExecutionRolePolicy

Descrizione: politica predefinita per il ruolo DataZone di DomainExecutionRole servizio di Amazon. Questo ruolo viene utilizzato da Amazon DataZone per catalogare, scoprire, gestire, condividere e analizzare i dati nel DataZone dominio Amazon.

AmazonDataZoneDomainExecutionRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneDomainExecutionRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 settembre 2023, 21:55 UTC
- Ora modificata: 01 aprile 2024, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListTimeSeriesDataPoints",
        "datazone:GetTimeSeriesDataPoint",
        "datazone>DeleteTimeSeriesDataPoints",
        "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" : "*"
}
]
}

```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

Descrizione: Amazon DataZone crea ruoli IAM for Environments per eseguire azioni di analisi dei dati e utilizza questa policy durante la creazione di questi ruoli per definire i limiti delle loro autorizzazioni.

AmazonDataZoneEnvironmentRolePermissionsBoundary è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneEnvironmentRolePermissionsBoundary ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 settembre 2023, 23:38 UTC
- Ora modificata: 17 novembre 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon DataZone tramite l'accesso limitato ai servizi correlati da esso richiesti. AWS Management Console

AmazonDataZoneFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 settembre 2023, 20:06 UTC
- Ora modificata: 23 aprile 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```

},
{
  "Sid" : "ReadOnlyStatement",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases",
    "iam:ListRoles",
    "sso:DescribeRegisteredRegions",
    "s3:ListAllMyBuckets",
    "redshift:DescribeClusters",
    "redshift-serverless:ListWorkgroups",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "secretsmanager:ListSecrets"
  ],
  "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" : "IAMGetPolicyStatement",
    "Effect" : "Allow",
    "Action" : "iam:GetPolicy",
    "Resource" : [
      "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
    ]
  },
  {
    "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_*"
      }
    }
  }
}

```

```
}  
  }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneFullUserAccess

Descrizione: fornisce l'accesso completo ad Amazon DataZone, ma non consente la gestione di domini, utenti o account associati.

AmazonDataZoneFullUserAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneFullUserAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 settembre 2023, 21:06 UTC
- Ora modificata: 01 aprile 2024, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:PostTimeSeriesDataPoints",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:GetTimeSeriesDataPoint",
        "datazone>DeleteTimeSeriesDataPoints",
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone>DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
        "datazone>DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone>DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone>DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone>DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",

```

```
"datazone:CreateListingChangeSet",
"datazone:DeleteListing",
"datazone:SearchListings",
"datazone:GetListing",
"datazone:CreateDataSource",
"datazone:GetDataSource",
"datazone:DeleteDataSource",
"datazone:UpdateDataSource",
"datazone:ListDataSources",
"datazone:StartDataSourceRun",
"datazone:GetDataSourceRun",
"datazone:ListDataSourceRuns",
"datazone:ListDataSourceRunActivities",
"datazone:ListEnvironmentBlueprintConfigurations",
"datazone:CreateEnvironmentBlueprint",
"datazone:GetEnvironmentBlueprint",
"datazone:DeleteEnvironmentBlueprint",
"datazone:UpdateEnvironmentBlueprint",
"datazone:ListEnvironmentBlueprints",
"datazone:CreateProject",
"datazone:UpdateProject",
"datazone:GetProject",
"datazone:DeleteProject",
"datazone:ListProjects",
"datazone:CreateProjectMembership",
"datazone:DeleteProjectMembership",
"datazone:ListProjectMemberships",
"datazone:CreateEnvironmentProfile",
"datazone:GetEnvironmentProfile",
"datazone:UpdateEnvironmentProfile",
"datazone:DeleteEnvironmentProfile",
"datazone:ListEnvironmentProfiles",
"datazone:CreateEnvironment",
"datazone:GetEnvironment",
"datazone:DeleteEnvironment",
"datazone:UpdateEnvironment",
"datazone:UpdateEnvironmentDeploymentStatus",
"datazone:ListEnvironments",
"datazone:ListAccountEnvironments",
"datazone:GetEnvironmentActionLink",
"datazone:GetEnvironmentCredentials",
"datazone:GetSubscriptionTarget",
"datazone:DeleteSubscriptionTarget",
"datazone:ListSubscriptionTargets",
```

```

        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone>DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone>DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "RAMResourceShareOperations",
    "Effect" : "Allow",
    "Action" : "ram:GetResourceShareAssociations",
    "Resource" : "*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneGlueManageAccessRolePolicy

Descrizione: la politica concede le autorizzazioni per consentire ad Amazon di DataZone abilitare la pubblicazione e le concessioni di accesso ai dati.

AmazonDataZoneGlueManageAccessRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneGlueManageAccessRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 settembre 2023, 20:21 UTC
- Ora modificata: 03 giugno 2024, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTagDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "glue:GetTags"
      ]
    }
  ],
}
```

```

    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      },
      "ForAnyValue:StringLikeIfExists" : {
        "aws:TagKeys" : "DataZoneDiscoverable_*"
      }
    }
  },
  {
    "Sid" : "GlueDataQualityPermissions",
    "Effect" : "Allow",
    "Action" : [
      "glue:ListDataQualityResults",
      "glue:GetDataQualityResult"
    ],
    "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "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:RegisterResource",
    "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"
    }
  }
},
{
  "Sid" : "GetRoleForDataZone",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],

```

```

    "Resource" : [
      "arn:aws:iam::*:role/AmazonDataZone*",
      "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
  },
  {
    "Sid" : "PassRoleForDataLocationRegistration",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AmazonDataZone*",
      "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lakeformation.amazonaws.com"
        ]
      }
    }
  }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZonePortalFullAccessPolicy

Descrizione: Fornisce accesso completo alle DataZone API di Amazon

AmazonDataZonePortalFullAccessPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZonePortalFullAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 marzo 2023, 18:24 UTC
- Ora modificata: 26 marzo 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZonePreviewConsoleFullAccess

Descrizione: fornisce l'accesso completo alla versione di anteprima di Amazon DataZone tramite AWS Management Console. Fornisce inoltre un accesso selezionato ad altri servizi correlati.

AmazonDataZonePreviewConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZonePreviewConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 marzo 2023, 15:16 UTC
- Ora modificata: 13 luglio 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

Descrizione: Amazon DataZone crea ruoli IAM che utilizza per distribuire progetti di analisi dei dati. DataZone utilizza questa politica durante la creazione di questi ruoli per definire i limiti delle relative autorizzazioni.

AmazonDataZoneProjectDeploymentPermissionsBoundary è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneProjectDeploymentPermissionsBoundary ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 marzo 2023, 02:54 UTC
- Ora modificata: 04 aprile 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneProjectRolePermissionsBoundary

Descrizione: Amazon DataZone crea ruoli IAM per i progetti per eseguire azioni di analisi dei dati e utilizza questa policy durante la creazione di questi ruoli per definire i limiti delle loro autorizzazioni.

AmazonDataZoneProjectRolePermissionsBoundary è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneProjectRolePermissionsBoundary ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 marzo 2023, 02:51 UTC

- Ora modificata: 21 marzo 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*",
"datzone:*"
],
```

```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

Descrizione: Amazon DataZone è un servizio di gestione dei dati che ti consente di catalogare, scoprire, governare, condividere e analizzare i tuoi dati. Con Amazon DataZone, puoi condividere e accedere ai tuoi dati tra account e regioni supportate. Amazon DataZone semplifica la tua esperienza con tutti AWS i servizi, tra cui, a titolo esemplificativo, Amazon Redshift, Amazon Athena, AWS Glue e Lake Formation. AWS

AmazonDataZoneRedshiftGlueProvisioningPolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneRedshiftGlueProvisioningPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 settembre 2023, 20:19 UTC
- Ora modificata: 12 marzo 2024, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "AmazonDataZoneEnvironmentKMSEncryptPermissions",
  "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*"
    }
  }
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

Descrizione: questa policy concede ad Amazon DataZone le autorizzazioni per pubblicare i dati di Amazon Redshift nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere o revocare l'accesso agli asset pubblicati di Amazon Redshift o Amazon Redshift Serverless nel catalogo.

AmazonDataZoneRedshiftManageAccessRolePolicy [AWS](#) è una politica gestita.

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneRedshiftManageAccessRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 settembre 2023, 20:15 UTC
- Ora modificata: 16 novembre 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Descrizione: la AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary policy è l'elenco delle autorizzazioni consentite su un ruolo di esecuzione creato in un SageMaker ambiente fornito da Amazon. DataZone

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2024, 23:01 UTC
- Ora modificata: 08 maggio 2024, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:*/*"
    },
    {
      "Sid" : "AllowLakeFormation",
      "Effect" : "Allow",
      "Action" : [
```

```

        "lakeformation:GetDataAccess"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowAddTagsForAppAndSpace",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:AddTags"
    ],
    "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "sagemaker:TaggingAction" : [
                "CreateApp",
                "CreateSpace"
            ]
        }
    }
},
{
    "Sid" : "AllowStudioActions",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListSpaces",
        "sagemaker:ListUserProfiles"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowAppActionsForUserProfile",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreateApp",

```

```

        "sagemaker:DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
    "Condition" : {
        "Null" : {
            "sagemaker:OwnerUserProfileArn" : "true"
        }
    }
},
{
    "Sid" : "AllowAppActionsForSharedSpaces",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*/*",
    "Condition" : {
        "StringEquals" : {
            "sagemaker:SpaceSharingType" : [
                "Shared"
            ]
        }
    }
},
{
    "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
        "Null" : {
            "sagemaker:OwnerUserProfileArn" : "true"
        }
    }
},
{
    "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
    "Effect" : "Allow",
    "Action" : [

```



```

        "sagemaker:CreateSpace",
        "sagemaker>DeleteSpace",
        "sagemaker:UpdateSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
        "ArnLike" : {
            "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
            "sagemaker:SpaceSharingType" : [
                "Private",
                "Shared"
            ]
        }
    }
},
{
    "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreateApp",
        "sagemaker>DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition" : {
        "ArnLike" : {
            "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
            "sagemaker:SpaceSharingType" : [
                "Private"
            ]
        }
    }
},
{
    "Sid" : "AllowFlowDefinitionActions",
    "Effect" : "Allow",
    "Action" : "sagemaker:*",
    "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
    ]
}

```

```

    ],
    "Condition" : {
      "StringEqualsIfExists" : {
        "sagemaker:WorkteamType" : [
          "private-crowd",
          "vendor-crowd"
        ]
      }
    }
  },
  {
    "Sid" : "AllowAWSServiceActions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:*",
      "datazone:*",
      "application-autoscaling:DeleteScalingPolicy",
      "application-autoscaling:DeleteScheduledAction",
      "application-autoscaling:DeregisterScalableTarget",
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingActivities",
      "application-autoscaling:DescribeScalingPolicies",
      "application-autoscaling:DescribeScheduledActions",
      "application-autoscaling:PutScalingPolicy",
      "application-autoscaling:PutScheduledAction",
      "application-autoscaling:RegisterScalableTarget",
      "aws-marketplace:ViewSubscriptions",
      "cloudformation:GetTemplateSummary",
      "cloudwatch:DeleteAlarms",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:GetMetricData",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:ListMetrics",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:PutMetricData",
      "codecommit:BatchGetRepositories",
      "codecommit:CreateRepository",
      "codecommit:GetRepository",
      "codecommit:List*",
      "ec2:CreateNetworkInterface",
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DescribeDhcpOptions",

```

```
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcs",
"ecr:BatchCheckLayerAvailability",
"ecr:BatchGetImage",
"ecr:Describe*",
"ecr:GetAuthorizationToken",
"ecr:GetDownloadUrlForLayer",
"ecr:StartImageScan",
"elastic-inference:Connect",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeMountTargets",
"fsx:DescribeFileSystems",
"groundtruthlabeling:*",
"iam:GetRole",
"iam:ListRoles",
"kms:DescribeKey",
"kms:ListAliases",
"lambda:ListFunctions",
"logs:CreateLogDelivery",
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs>DeleteLogDelivery",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:GetLogDelivery",
"logs:GetLogEvents",
"logs:ListLogDeliveries",
"logs:PutLogEvents",
"logs:UpdateLogDelivery",
"redshift-data:BatchExecuteStatement",
"redshift-data:CancelStatement",
"redshift-data:DescribeStatement",
"redshift-data:DescribeTable",
"redshift-data:ExecuteStatement",
"redshift-data:GetStatementResult",
"redshift-data:ListSchemas",
"redshift-data:ListTables",
"redshift-serverless:GetCredentials",
"redshift-serverless:GetNamespace",
```

```

        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowRAMInvitation",
    "Effect" : "Allow",
    "Action" : "ram:AcceptResourceShareInvitation",
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ram:ResourceShareName" : "dzd_*"
        }
    }
},
{
    "Sid" : "AllowECRActions",
    "Effect" : "Allow",
    "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr>DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr>DeleteRepository",
        "ecr:PutImage",
        "ecr:TagResource",
        "ecr:UntagResource"
    ],
    "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker*",
        "arn:aws:ecr:*:*:repository/datazone*"
    ]
}

```

```

    ]
  },
  {
    "Sid" : "AllowCodeCommitActions",
    "Effect" : "Allow",
    "Action" : [
      "codecommit:GitPull",
      "codecommit:GitPush"
    ],
    "Resource" : [
      "arn:aws:codecommit:*:*:*sagemaker*",
      "arn:aws:codecommit:*:*:*SageMaker*",
      "arn:aws:codecommit:*:*:*Sagemaker*"
    ]
  },
  {
    "Sid" : "AllowCodeBuildActions",
    "Action" : [
      "codebuild:BatchGetBuilds",
      "codebuild:StartBuild"
    ],
    "Resource" : [
      "arn:aws:codebuild:*:*:project/sagemaker*",
      "arn:aws:codebuild:*:*:build/*"
    ],
    "Effect" : "Allow"
  },
  {
    "Sid" : "AllowStepFunctionsActions",
    "Action" : [
      "states:DescribeExecution",
      "states:GetExecutionHistory",
      "states:StartExecution",
      "states:StopExecution",
      "states:UpdateStateMachine"
    ],
    "Resource" : [
      "arn:aws:states:*:*:statemachine:*sagemaker*",
      "arn:aws:states:*:*:execution:*sagemaker*:*"
    ],
    "Effect" : "Allow"
  },
  {
    "Sid" : "AllowSecretManagerActions",

```

```

    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
    ],
    "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    ]
},
{
    "Sid" : "AllowServiceCatalogProvisionProduct",
    "Effect" : "Allow",
    "Action" : [
        "servicecatalog:ProvisionProduct"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
    "Effect" : "Allow",
    "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "servicecatalog:userLevel" : "self"
        }
    }
},
{
    "Sid" : "AllowS3ObjectActions",
    "Effect" : "Allow",
    "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",

```

```

        "s3:RestoreObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
    ],
    "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
    ]
},
{
    "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::*"
    ],
    "Condition" : {
        "StringEqualsIgnoreCase" : {
            "s3:ExistingObjectTag/SageMaker" : "true"
        }
    }
},
{
    "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::*"
    ],
    "Condition" : {
        "StringEquals" : {
            "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
    }
},

```

```

{
  "Sid" : "AllowS3BucketActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors"
  ],
  "Resource" : [
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::Sagemaker-DataZone*",
    "arn:aws:s3:::DataZone-Sagemaker*",
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
  ]
},
{
  "Sid" : "ReadSageMakerJumpstartArtifacts",
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : [
    "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
  ]
},
{
  "Sid" : "AllowLambdaInvokeFunction",
  "Effect" : "Allow",
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : [

```



```

        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
    ]
},
{
    "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
    "Action" : "iam:CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/sagemaker.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
    }
},
{
    "Sid" : "AllowSNSActions",
    "Effect" : "Allow",
    "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
    ],
    "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
    ]
},
{
    "Sid" : "AllowPassRoleForSageMakerRoles",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [

```

```

        "glue.amazonaws.com",
        "bedrock.amazonaws.com",
        "states.amazonaws.com",
        "lakeformation.amazonaws.com",
        "events.amazonaws.com",
        "sagemaker.amazonaws.com",
        "forecast.amazonaws.com"
    ]
}
},
{
    "Sid" : "CrossAccountKmsOperations",
    "Effect" : "Allow",
    "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringNotEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "KmsOperationsWithResourceTag",
    "Effect" : "Allow",
    "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
    }
},

```

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

```

    "athena:UpdatePreparedStatement"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowGlueCreateDatabase",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default"
  ]
},
{
  "Sid" : "AllowRedshiftGetClusterCredentials",
  "Effect" : "Allow",
  "Action" : [
    "redshift:GetClusterCredentials"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
  ]
},
{
  "Sid" : "AllowListTags",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListTags"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:user-profile/*",
    "arn:aws:sagemaker:*:*:domain/*"
  ]
},
{
  "Sid" : "AllowCloudformationListStackResources",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ListStackResources"
  ]
}

```

```
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
  },
  {
    "Sid" : "AllowGlueActions",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetColumnStatisticsForPartition",
      "glue:GetColumnStatisticsForTable",
      "glue:ListJobs",
      "glue:CreateSession",
      "glue:RunStatement",
      "glue:BatchCreatePartition",
      "glue:CreatePartitionIndex",
      "glue:CreateTable",
      "glue:BatchGetWorkflows",
      "glue:BatchUpdatePartition",
      "glue:BatchDeletePartition",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:UpdateTable",
      "glue>DeleteTableVersion",
      "glue>DeleteTable",
      "glue>DeleteColumnStatisticsForPartition",
      "glue>DeleteColumnStatisticsForTable",
      "glue>DeletePartitionIndex",
      "glue:UpdateColumnStatisticsForPartition",
      "glue:UpdateColumnStatisticsForTable",
      "glue:BatchDeleteTableVersion",
      "glue:BatchDeleteTable",
      "glue:CreatePartition",
      "glue>DeletePartition",
      "glue:UpdatePartition",
      "glue:CreateBlueprint",
      "glue:CreateJob",
      "glue:CreateConnection",
      "glue:CreateCrawler",
      "glue:CreateDataQualityRuleset",
      "glue:CreateWorkflow",
      "glue:GetDatabases",
      "glue:GetTables",
      "glue:GetTable",
      "glue:SearchTables",
      "glue:NotifyEvent",
    ]
  }
}
```

```
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
        "glue:GetDatabase"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "AllowGlueActionsWithEnvironmentTag",
    "Effect" : "Allow",
    "Action" : [
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue>DeleteJob",
        "glue>DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue>DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:ListSchemas",
        "glue>DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:UpdateCrawlerSchedule",
        "glue>DeleteConnection",
        "glue:UpdateConnection",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions",
```

```

        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*"
    ],
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
    }
},
{
    "Sid" : "AllowGlueDefaultAccess",
    "Effect" : "Allow",
    "Action" : [
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:RunStatement"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:connection/dz-sm-*",
        "arn:aws:glue:*:*:session/*"
    ]
},
{
    "Sid" : "AllowRedshiftClusterActions",
    "Effect" : "Allow",
    "Action" : [
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters"
    ],
    "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
    ]
},
{
    "Sid" : "AllowCreateClusterUser",

```

```

    "Effect" : "Allow",
    "Action" : [
        "redshift:CreateClusterUser"
    ],
    "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
    ]
},
{
    "Sid" : "AllowCreateSecretActions",
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*",
            "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
        },
        "Null" : {
            "aws:TagKeys" : "false",
            "aws:ResourceTag/AmazonDataZoneProject" : "false",
            "aws:ResourceTag/AmazonDataZoneDomain" : "false",
            "aws:RequestTag/AmazonDataZoneDomain" : "false",
            "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "AmazonDataZoneDomain",
                "AmazonDataZoneProject"
            ]
        }
    }
},
{
    "Sid" : "ForecastOperations",
    "Effect" : "Allow",
    "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",

```



```

        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast>DeleteResourceTree"
    ],
    "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
    ]
},
{
    "Sid" : "RDSOperation",
    "Effect" : "Allow",
    "Action" : "rds:DescribeDBInstances",
    "Resource" : "*"
},
{
    "Sid" : "AllowEventBridgeRule",
    "Effect" : "Allow",
    "Action" : [
        "events:PutRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
    }
}

```

```

    }
  },
  {
    "Sid" : "EventBridgeOperations",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:PutTargets"
    ],
    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
      }
    }
  },
  {
    "Sid" : "EventBridgeTagBasedOperations",
    "Effect" : "Allow",
    "Action" : [
      "events:TagResource"
    ],
    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
        "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
      }
    }
  },
  {
    "Sid" : "EventBridgeListTagOperation",
    "Effect" : "Allow",
    "Action" : "events:ListTagsForResource",
    "Resource" : "*"
  },
  {
    "Sid" : "AllowEMR",
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:DescribeCluster",
      "elasticmapreduce:ListInstanceGroups",
      "elasticmapreduce:ListClusters"
    ],
  },

```

```

    "Resource" : "*"
  },
  {
    "Sid" : "AllowSSOAction",
    "Effect" : "Allow",
    "Action" : [
      "sso:CreateApplicationAssignment",
      "sso:AssociateProfile"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DenyNotAction",
    "Effect" : "Deny",
    "NotAction" : [
      "sagemaker:*",
      "sagemaker-geospatial:*",
      "sqlworkbench:*",
      "datazone:*",
      "forecast:*",
      "application-autoscaling:DeleteScalingPolicy",
      "application-autoscaling:DeleteScheduledAction",
      "application-autoscaling:DeregisterScalableTarget",
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingActivities",
      "application-autoscaling:DescribeScalingPolicies",
      "application-autoscaling:DescribeScheduledActions",
      "application-autoscaling:PutScalingPolicy",
      "application-autoscaling:PutScheduledAction",
      "application-autoscaling:RegisterScalableTarget",
      "athena:BatchGetNamedQuery",
      "athena:BatchGetPreparedStatement",
      "athena:BatchGetQueryExecution",
      "athena:CreateNamedQuery",
      "athena:CreateNotebook",
      "athena:CreatePreparedStatement",
      "athena:CreatePresignedNotebookUrl",
      "athena>DeleteNamedQuery",
      "athena>DeleteNotebook",
      "athena>DeletePreparedStatement",
      "athena:ExportNotebook",
      "athena:GetDatabase",
      "athena:GetDataCatalog",
      "athena:GetNamedQuery",

```

```
"athena:GetPreparedStatement",
"athena:GetQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryResultsStream",
"athena:GetQueryRuntimeStatistics",
"athena:GetTableMetadata",
"athena:GetWorkGroup",
"athena:ImportNotebook",
"athena:ListDatabases",
"athena:ListDataCatalogs",
"athena:ListEngineVersions",
"athena:ListNamedQueries",
"athena:ListPreparedStatements",
"athena:ListQueryExecutions",
"athena:ListTableMetadata",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"athena:StartCalculationExecution",
"athena:StartQueryExecution",
"athena:StartSession",
"athena:StopCalculationExecution",
"athena:StopQueryExecution",
"athena:TerminateSession",
"athena:UpdateNamedQuery",
"athena:UpdateNotebook",
"athena:UpdateNotebookMetadata",
"athena:UpdatePreparedStatement",
"aws-marketplace:ViewSubscriptions",
"cloudformation:GetTemplateSummary",
"cloudformation:ListStackResources",
"cloudwatch:DeleteAlarms",
"cloudwatch:DescribeAlarms",
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"cloudwatch:PutMetricAlarm",
"cloudwatch:PutMetricData",
"codebuild:BatchGetBuilds",
"codebuild:StartBuild",
"codecommit:BatchGetRepositories",
"codecommit:CreateRepository",
"codecommit:GetRepository",
"codecommit:List*",
"codecommit:GitPull",
```

```
"codecommit:GitPush",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:DeleteNetworkInterface",
"ec2:DeleteNetworkInterfacePermission",
"ec2:DescribeDhcpOptions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcs",
"ecr:BatchCheckLayerAvailability",
"ecr:BatchGetImage",
"ecr:CreateRepository",
"ecr:Describe*",
"ecr:GetAuthorizationToken",
"ecr:GetDownloadUrlForLayer",
"ecr:SetRepositoryPolicy",
"ecr:CompleteLayerUpload",
"ecr:BatchDeleteImage",
"ecr:UploadLayerPart",
"ecr:DeleteRepositoryPolicy",
"ecr:InitiateLayerUpload",
"ecr:DeleteRepository",
"ecr:PutImage",
"ecr:StartImageScan",
"ecr:TagResource",
"ecr:UntagResource",
"elastic-inference:Connect",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeMountTargets",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:ListInstanceGroups",
"elasticmapreduce:ListClusters",
"events:PutRule",
"events:DescribeRule",
"events:PutTargets",
"events:TagResource",
"events:ListTagsForResource",
"fsx:DescribeFileSystems",
"glue:SearchTables",
"glue:NotifyEvent",
```

```
"glue:StartBlueprintRun",
"glue:PutWorkflowRunProperties",
"glue:StopCrawler",
"glue:DeleteJob",
"glue:DeleteWorkflow",
"glue:UpdateCrawler",
"glue:DeleteBlueprint",
"glue:UpdateWorkflow",
"glue:StartCrawler",
"glue:ResetJobBookmark",
"glue:UpdateJob",
"glue:StartWorkflowRun",
"glue:StopCrawlerSchedule",
"glue:ResumeWorkflowRun",
"glue:DeleteCrawler",
"glue:UpdateBlueprint",
"glue:BatchStopJobRun",
"glue:StopWorkflowRun",
"glue:BatchGet*",
"glue:UpdateCrawlerSchedule",
"glue:DeleteConnection",
"glue:UpdateConnection",
"glue:Get*",
"glue:BatchDeleteConnection",
"glue:StartCrawlerSchedule",
"glue:StartJobRun",
"glue:CreateWorkflow",
"glue:*DataQuality*",
"glue:List*",
"glue:CreateSession",
"glue:RunStatement",
"glue:BatchCreatePartition",
"glue:CreateDatabase",
"glue:CreatePartitionIndex",
"glue:CreateTable",
"glue:BatchUpdatePartition",
"glue:BatchDeletePartition",
"glue:UpdateTable",
"glue:DeleteTableVersion",
"glue:DeleteTable",
"glue:DeleteColumnStatisticsForPartition",
"glue:DeleteColumnStatisticsForTable",
"glue:DeletePartitionIndex",
"glue:UpdateColumnStatisticsForPartition",
```

```
"glue:UpdateColumnStatisticsForTable",
"glue:BatchDeleteTableVersion",
"glue:BatchDeleteTable",
"glue:CreatePartition",
"glue>DeletePartition",
"glue:UpdatePartition",
"glue:CreateBlueprint",
"glue:CreateJob",
"glue:CreateConnection",
"glue:CreateCrawler",
"groundtruthlabeling:*",
"iam:CreateServiceLinkedRole",
"iam:GetRole",
"iam:ListRoles",
"iam:PassRole",
"kms:DescribeKey",
"kms:ListAliases",
"kms:Decrypt",
"kms:ListKeys",
"kms:Encrypt",
"kms:GenerateDataKey",
"kms:RetireGrant",
"lakeformation:GetDataAccess",
"lambda:ListFunctions",
"lambda:InvokeFunction",
"logs:CreateLogDelivery",
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs>DeleteLogDelivery",
"logs:Describe*",
"logs:GetLogDelivery",
"logs:GetLogEvents",
"logs:ListLogDeliveries",
"logs:PutLogEvents",
"logs:UpdateLogDelivery",
"ram:AcceptResourceShareInvitation",
"rds:DescribeDBInstances",
"redshift:CreateClusterUser",
"redshift:GetClusterCredentials",
"redshift:GetClusterCredentialsWithIAM",
"redshift:DescribeClusters",
"redshift-data:BatchExecuteStatement",
"redshift-data:CancelStatement",
"redshift-data:DescribeStatement",
```

```
"redshift-data:DescribeTable",
"redshift-data:ExecuteStatement",
"redshift-data:GetStatementResult",
"redshift-data:ListSchemas",
"redshift-data:ListTables",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListWorkgroups",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:GetCredentials",
"s3:GetBucketAcl",
"s3:PutObjectAcl",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:AbortMultipartUpload",
"s3:CreateBucket",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:ListAllMyBuckets",
"s3:GetBucketCors",
"s3:PutBucketCors",
"s3:DeleteObjectVersion",
"s3:PutObjectRetention",
"s3:ReplicateObject",
"s3:RestoreObject",
"secretsmanager:ListSecrets",
"secretsmanager:DescribeSecret",
"secretsmanager:GetSecretValue",
"secretsmanager:CreateSecret",
"secretsmanager:PutResourcePolicy",
"secretsmanager:TagResource",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"servicecatalog:ProvisionProduct",
"servicecatalog:TerminateProvisionedProduct",
"servicecatalog:UpdateProvisionedProduct",
"sns:ListTopics",
"sns:Subscribe",
"sns:CreateTopic",
"sns:Publish",
```



```
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine",
    "tag:GetResources",
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneSageMakerManageAccessRolePolicy

Descrizione: la AmazonDataZoneSageMakerManageAccessRolePolicy policy concede ad Amazon DataZone le autorizzazioni necessarie per concedere agli utenti l'accesso a varie risorse dell' SageMaker ambiente.

AmazonDataZoneSageMakerManageAccessRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneSageMakerManageAccessRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2024, 23:34 UTC
- Ora modificata: 23 aprile 2024, 23:34 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
```

```

        "aws:TagKeys" : [
            "sagemaker:shared-with:*"
        ]
    }
},
{
    "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker>DeleteModelPackageGroupPolicy"
    ],
    "Resource" : [
        "arn:*:sagemaker:*:*:model-package-group/*"
    ]
},
{
    "Sid" : "AmazonSageMakerRAMPermission",
    "Effect" : "Allow",
    "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:PutResourcePolicy",
        "sagemaker:GetResourcePolicy",
        "sagemaker>DeleteResourcePolicy"
    ],
    "Resource" : [
        "arn:*:sagemaker:*:*:feature-group/*"
    ]
},
{
    "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
    "Effect" : "Allow",
    "Action" : [
        "ram:TagResource"
    ]
}

```

```

    ],
    "Resource" : "arn:*:ram:*:*:resource-share/*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
    }
},
{
    "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
    "Effect" : "Allow",
    "Action" : [
        "ram:DeleteResourceShare"
    ],
    "Resource" : "arn:*:ram:*:*:resource-share/*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/AwsDataZoneDomainId" : "false"
        }
    }
},
{
    "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
    "Effect" : "Allow",
    "Action" : [
        "ram:CreateResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLikeIfExists" : {
            "ram:RequestedResourceType" : [
                "sagemaker:*"
            ]
        },
        "Null" : {
            "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
    }
},
{
    "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
    "Effect" : "Allow",
    "Action" : [
        "s3:DeleteBucketPolicy",

```

```

        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
    ],
    "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*"
    ]
},
{
    "Sid" : "AmazonSageMakerS3Permission",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*"
    ]
},
{
    "Sid" : "AmazonSageMakerECRPermission",
    "Effect" : "Allow",
    "Action" : [
        "ecr:GetRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "ecr>DeleteRepositoryPolicy"
    ],
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
    }
},
{
    "Sid" : "AmazonSageMakerKMSReadPermission",
    "Effect" : "Allow",

```

```
"Action" : [
  "kms:DescribeKey"
],
"Resource" : "*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:TagKeys" : [
      "AmazonDataZoneEnvironment"
    ]
  }
},
{
  "Sid" : "AmazonSageMakerKMSGrantPermission",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "AmazonDataZoneEnvironment"
      ]
    },
    "ForAllValues:StringEquals" : {
      "kms:GrantOperations" : [
        "Decrypt"
      ]
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDataZoneSageMakerProvisioningRolePolicy

Descrizione: la AmazonDataZoneSageMakerProvisioningRolePolicy politica concede ad Amazon DataZone le autorizzazioni necessarie per interagire con Amazon. SageMaker

AmazonDataZoneSageMakerProvisioningRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonDataZoneSageMakerProvisioningRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2024, 23:32 UTC
- Ora modificata: 23 aprile 2024, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```

    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      },
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "AmazonDataZoneEnvironment"
        ]
      },
      "Null" : {
        "aws:TagKeys" : "false",
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
        "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
      }
    }
  },
  {
    "Sid" : "DeleteSageMakerStudio",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:DeleteDomain"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      },
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : [
          "AmazonDataZoneEnvironment"
        ]
      },
      "Null" : {
        "aws:TagKeys" : "false",
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
      }
    }
  }
}

```



```

    }
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:DescribeDomain"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "IamPassRolePermissions",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com",
          "lakeformation.amazonaws.com",
          "sagemaker.amazonaws.com"
        ],
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
    "Effect" : "Allow",
    "Action" : [

```

```

        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam>DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:CalledViaFirst" : [
                "cloudformation.amazonaws.com"
            ],
            "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
    },
    {
        "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
        "Effect" : "Allow",
        "Action" : [
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam>DeleteRole"
        ],
        "Resource" : [
            "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
        ],
        "Condition" : {
            "StringEquals" : {
                "aws:CalledViaFirst" : [
                    "cloudformation.amazonaws.com"
                ]
            }
        }
    },
    {
        "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
        "Effect" : "Allow",
        "Action" : [
            "iam:CreateServiceLinkedRole"
        ],

```

```

    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "sagemaker:ListDomains"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey"
    ],
    "Resource" : "arn:aws:kms::*:key/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
      }
    }
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateConnection",
      "glue>DeleteConnection"
    ],
    "Resource" : [
      "arn:aws:glue::*:connection/dz-sm-athena-glue-connection-*",

```

```
    "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
    "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
    "arn:aws:glue:*:*:catalog"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDetectiveFullAccess

Descrizione: Fornisce accesso completo al servizio Amazon Detective e accesso mirato alle dipendenze dell'interfaccia utente della console

AmazonDetectiveFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDetectiveFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 aprile 2020, 17:57 UTC
- Ora modificata: 17 maggio 2023, 19:39 UTC

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

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"   
}   
]   
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDetectiveInvestigatorAccess

Descrizione: fornisce agli investigatori l'accesso al servizio Amazon Detective e l'accesso mirato alle dipendenze dell'interfaccia utente della console. Questa politica concede il permesso di immergersi in Detective per scopi investigativi e un accesso scritto limitato a Guardduty.

AmazonDetectiveInvestigatorAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDetectiveInvestigatorAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 gennaio 2023, 15:24 UTC
- Ora modificata: 27 novembre 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDetectiveMemberAccess

Descrizione: fornisce ai membri l'accesso al servizio Amazon Detective e l'accesso mirato alle dipendenze dell'interfaccia utente della console.

AmazonDetectiveMemberAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonDetectiveMemberAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 gennaio 2023, 15:16 UTC
- Ora modificata: 17 gennaio 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDetectiveOrganizationsAccess

Descrizione: Fornisce alle Organizzazioni l'accesso alla gestione dell'amministratore delegato per Amazon Detective e l'accesso mirato alle dipendenze dell'interfaccia utente della console. Ciò concede anche l'autorizzazione a creare un ruolo collegato al servizio per Detective.

AmazonDetectiveOrganizationsAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonDetectiveOrganizationsAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 marzo 2023, 15:20 UTC
- Ora modificata: 2 marzo 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Effect" : "Allow",
"Action" : [
  "organizations:DescribeAccount",
  "organizations:DescribeOrganization",
  "organizations:ListAccounts"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "detective.amazonaws.com",
        "guardduty.amazonaws.com",
        "macie.amazonaws.com",
        "securityhub.amazonaws.com"
      ]
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDetectiveServiceLinkedRolePolicy

Descrizione: consente ad Amazon Detective di effettuare chiamate di assistenza per tuo conto

AmazonDetectiveServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 novembre 2021, 19:47 UTC
- Ora modificata: 18 novembre 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDevOpsGuruConsoleFullAccess

Descrizione: la policy garantisce l'accesso completo alla console DevOps Guru.

AmazonDevOpsGuruConsoleFullAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonDevOpsGuruConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 dicembre 2021, 18:43 UTC
- Ora modificata: 25 agosto 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDevOpsGuruFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon DevOps Guru.

AmazonDevOpsGuruFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDevOpsGuruFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 16:38 UTC
- Ora modificata: 25 agosto 2022, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDevOpsGuruOrganizationsAccess

Descrizione: Fornisci l'accesso per abilitare e gestire Amazon DevOps Guru all'interno di un'organizzazione.

AmazonDevOpsGuruOrganizationsAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDevOpsGuruOrganizationsAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2021, 23:50 UTC
- Ora modificata: 15 novembre 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDevOpsGuruReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura alla console Amazon DevOps Guru.

AmazonDevOpsGuruReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDevOpsGuruReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 16:34 UTC

- Ora modificata: 25 agosto 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}

```



```
}  
  }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDevOpsGuruServiceRolePolicy

Descrizione: un ruolo collegato al servizio richiesto ad Amazon DevOpsGuru per accedere alle tue risorse.

AmazonDevOpsGuruServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 01 dicembre 2020, 10:24 UTC
- Ora modificata: 10 gennaio 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  ]
}

```

```
]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDMSCloudWatchLogsRole

Descrizione: fornisce l'accesso per caricare i log di replica DMS sui log di cloudwatch nell'account del cliente.

AmazonDMSCloudWatchLogsRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonDMSCloudWatchLogsRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 gennaio 2016, 23:44 UTC
- Ora modificata: 23 maggio 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDMSRedshiftS3Role

Descrizione: fornisce l'accesso per gestire le impostazioni S3 per gli endpoint Redshift per DMS.

AmazonDMSRedshiftS3Role è [una policy gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonDMSRedshiftS3Role ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2016, 17:05 UTC
- Ora modificata: 08 luglio 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDMSVPCManagementRole

Descrizione: Fornisce l'accesso alla gestione delle impostazioni VPC per le configurazioni AWS gestite dei clienti

AmazonDMSVPCManagementRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDMSVPCManagementRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 novembre 2015, 16:33 UTC
- Ora modificata: 23 maggio 2016, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDocDB-ElasticServiceRolePolicy

Descrizione: consente ad Amazon DocumentDB-Elastic di gestire AWS le risorse per tuo conto.

AmazonDocDB-ElasticServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 novembre 2022, 14:17 UTC
- Ora modificata: 30 novembre 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDocDBConsoleFullAccess

Descrizione: fornisce l'accesso completo alla gestione di Amazon DocumentDB con compatibilità con MongoDB utilizzando. AWS Management Console Tieni presente che questa politica garantisce anche l'accesso completo alla pubblicazione su tutti gli argomenti SNS all'interno dell'account, le

autorizzazioni per creare e modificare istanze Amazon EC2 e configurazioni VPC, le autorizzazioni per visualizzare ed elencare le chiavi su Amazon KMS e l'accesso completo ad Amazon RDS e Amazon Neptune.

AmazonDocDBConsoleFullAccess è una [AWS politica](#) gestita.

Utilizzo di questa politica

Puoi collegarti AmazonDocDBConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 gennaio 2019, 20:37 UTC
- Ora modificata: 30 novembre 2022, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:RemoveTagsForResource",
        "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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDocDBElasticFullAccess

Descrizione: fornisce l'accesso completo ad Amazon DocumentDB Elastic Clusters e ad altre autorizzazioni richieste per le sue dipendenze, tra cui EC2, KMS e IAM. SecretsManager CloudWatch

AmazonDocDBElasticFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonDocDBElasticFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 giugno 2023, 13:51 UTC
- Ora modificata: 21 giugno 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDocDBElasticReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon DocDB-Elastic e ai parametri. CloudWatch

AmazonDocDBElasticReadOnlyAccess [AWS è una](#) politica gestita.

Utilizzo di questa politica

Puoi collegarti AmazonDocDBElasticReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 giugno 2023, 14:37 UTC
- Ora modificata: 21 giugno 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDocDBFullAccess

Descrizione: fornisce l'accesso completo ad Amazon DocumentDB con compatibilità con MongoDB. Tieni presente che questa politica garantisce anche l'accesso completo alla pubblicazione su tutti gli argomenti SNS all'interno dell'account e l'accesso completo ad Amazon RDS e Amazon Neptune.

AmazonDocDBFullAccess [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonDocDBFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 gennaio 2019, 20:21 UTC
- Ora modificata: 09 gennaio 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:RemoveTagsForResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
    ],
    "Effect" : "Allow",
    "Resource" : [
        "*"
    ]
},
{
    "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",

```

```

        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
    ],
    "Effect" : "Allow",
    "Resource" : [
        "*"
    ]
},
{
    "Action" : "iam:CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "rds.amazonaws.com"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDocDBReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon DocumentDB con compatibilità con MongoDB. Tieni presente che questa politica consente anche l'accesso alle risorse di Amazon RDS e Amazon Neptune.

AmazonDocDBReadOnlyAccess [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonDocDBReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 gennaio 2019, 20:30 UTC
- Ora modificata: 09 gennaio 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDRSVPCManagement

Descrizione: Fornisce l'accesso per gestire le impostazioni VPC per le configurazioni gestite dai clienti di Amazon

AmazonDRSVPCManagement è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDRSVPCManagement ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 settembre 2015, 00:09 UTC
- Ora modificata: 02 settembre 2015, 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDynamoDBFullAccess

Descrizione: fornisce l'accesso completo ad Amazon DynamoDB tramite AWS Management Console

AmazonDynamoDBFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDynamoDBFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 29 gennaio 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"  
      ]  
    }  
  }  
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDynamoDBFullAccesswithDataPipeline

Descrizione: questa politica si trova su un percorso obsoleto. Consulta la documentazione come guida: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>. Fornisce accesso completo ad Amazon DynamoDB, incluso Export/Import AWS using Data Pipeline tramite. AWS Management Console

AmazonDynamoDBFullAccesswithDataPipeline [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonDynamoDBFullAccesswithDataPipeline ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 12 novembre 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonDynamoDBReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon DynamoDB tramite. AWS Management Console

AmazonDynamoDBReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonDynamoDBReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 20 marzo 2024, 15:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEBSCSIDriverPolicy

Descrizione: politica IAM che consente all'account del servizio driver CSI di effettuare chiamate a servizi correlati come EC2 per tuo conto.

AmazonEBSCSIDriverPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEBSCSIDriverPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 4 aprile 2022, 17:24 UTC
- Ora modificata: 18 novembre 2022, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2ContainerRegistryFullAccess

Descrizione: Fornisce accesso amministrativo alle risorse Amazon ECR

AmazonEC2ContainerRegistryFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2ContainerRegistryFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 dicembre 2015, 17:06 UTC
- Ora modificata: 05 dicembre 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2ContainerRegistryPowerUser

Descrizione: fornisce l'accesso completo ai repository di Amazon EC2 Container Registry, ma non consente l'eliminazione degli archivi o la modifica delle policy.

AmazonEC2ContainerRegistryPowerUser [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2ContainerRegistryPowerUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 dicembre 2015, 17:05 UTC
- Ora modificata: 10 dicembre 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2ContainerRegistryReadOnly

Descrizione: fornisce accesso in sola lettura ai repository di Amazon EC2 Container Registry.

AmazonEC2ContainerRegistryReadOnly è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonEC2ContainerRegistryReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 dicembre 2015, 17:04 UTC
- Ora modificata: 10 dicembre 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2ContainerServiceAutoscaleRole

Descrizione: policy per abilitare Task Autoscaling per Amazon EC2 Container Service

AmazonEC2ContainerServiceAutoscaleRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonEC2ContainerServiceAutoscaleRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 maggio 2016, 23:25 UTC
- Ora modificata: 5 febbraio 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2ContainerServiceEventsRole

Descrizione: Politica per abilitare CloudWatch Events for EC2 Container Service

AmazonEC2ContainerServiceEventsRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2ContainerServiceEventsRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 30 maggio 2017, 16:51 UTC
- Ora modificata: 6 marzo 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
}
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2ContainerServiceforEC2Role

Descrizione: policy predefinita per il ruolo Amazon EC2 per Amazon EC2 Container Service.

AmazonEC2ContainerServiceforEC2Role è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2ContainerServiceforEC2Role ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 marzo 2015, 18:45 UTC
- Ora modificata: 6 marzo 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2ContainerServiceRole

Descrizione: policy predefinita per il ruolo del servizio Amazon ECS.

AmazonEC2ContainerServiceRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2ContainerServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 9 aprile 2015, 16:14 UTC
- Ora modificata: 11 agosto 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2FullAccess

Descrizione: fornisce l'accesso completo ad Amazon EC2 tramite AWS Management Console

AmazonEC2FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 27 novembre 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2ReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EC2 tramite AWS Management Console

AmazonEC2ReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 14 febbraio 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2RoleforAWSCodeDeploy

Descrizione: fornisce l'accesso EC2 al bucket S3 per scaricare la revisione. Questo ruolo è necessario all' CodeDeploy agente sulle istanze EC2.

AmazonEC2RoleforAWSCodeDeploy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2RoleforAWSCodeDeploy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 maggio 2015, 18:10 UTC

- Ora modificata: 20 marzo 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2RoleforAWSCodeDeployLimited

Descrizione: fornisce a EC2 un accesso limitato al bucket S3 per scaricare la revisione. Questo ruolo è necessario all' CodeDeploy agente sulle istanze EC2.

AmazonEC2RoleforAWSCodeDeployLimited è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2RoleforAWSCodeDeployLimited ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 agosto 2020, 17:55 UTC
- Ora modificata: 20 gennaio 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2RoleforDataPipelineRole

Descrizione: policy predefinita per il ruolo del servizio Amazon EC2 Role for Data Pipeline.

AmazonEC2RoleforDataPipelineRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2RoleforDataPipelineRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC

- Ora modificata: 22 febbraio 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2RoleforSSM

Descrizione: questa politica sarà presto obsoleta. Utilizza la ManagedInstanceCore policy di AmazonSSM per abilitare le funzionalità principali del servizio AWS Systems Manager sulle istanze EC2. Per ulteriori informazioni, consulta <https://docs.aws.amazon.com/systems-manager/latest/userguide/.html> setup-instance-profile

AmazonEC2RoleforSSM è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2RoleforSSM ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 maggio 2015, 17:48 UTC
- Ora modificata: 24 gennaio 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2RolePolicyForLaunchWizard

Descrizione: policy gestita per il ruolo LaunchWizard di servizio Amazon per EC2

AmazonEC2RolePolicyForLaunchWizard è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2RolePolicyForLaunchWizard ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 08:05 UTC
- Ora modificata: 16 maggio 2022, 21:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2SpotFleetAutoscaleRole

Descrizione: Policy per abilitare la scalabilità automatica per la flotta Spot di Amazon EC2

AmazonEC2SpotFleetAutoscaleRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonEC2SpotFleetAutoscaleRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 agosto 2016, 18:27 UTC
- Ora modificata: 18 febbraio 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEC2SpotFleetTaggingRole

Descrizione: consente a EC2 Spot Fleet di richiedere, terminare e contrassegnare istanze Spot per tuo conto.

AmazonEC2SpotFleetTaggingRole è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonEC2SpotFleetTaggingRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 giugno 2017, 18:19 UTC
- Ora modificata: 23 aprile 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*/*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonECS_FullAccess

Descrizione: fornisce l'accesso amministrativo alle risorse di Amazon ECS e abilita le funzionalità ECS tramite l'accesso ad altre risorse di AWS servizio, tra cui VPC, gruppi di Auto Scaling e stack CloudFormation

AmazonECS_FullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonECS_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 novembre 2017, 21:36 UTC
- Ora modificata: 04 gennaio 2023, 16:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Versione della politica

Versione della politica: v20 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

Descrizione: Fornisce l'accesso amministrativo a Private Certificate Authority, AWS Secrets Manager e ad altri elementi Servizi AWS necessari per gestire le funzionalità TLS di ECS Service Connect per tuo conto.

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 gennaio 2024, 20:08 UTC
- Ora modificata: 19 gennaio 2024, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/AmazonECManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        }
      }
    }
  ]
}
```

```

        "StringEquals" : {
            "aws:RequestTag/AmazonECSManaged" : "true",
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    },
    {
        "Sid" : "RotateTLSCertificateSecret",
        "Effect" : "Allow",
        "Action" : [
            "secretsmanager:DescribeSecret",
            "secretsmanager:UpdateSecret",
            "secretsmanager:GetSecretValue",
            "secretsmanager:PutSecretValue",
            "secretsmanager>DeleteSecret",
            "secretsmanager:RotateSecret",
            "secretsmanager:UpdateSecretVersionStage"
        ],
        "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
        "Condition" : {
            "StringEquals" : {
                "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
                "aws:ResourceAccount" : "${aws:PrincipalAccount}"
            }
        }
    },
    {
        "Sid" : "ManagePrivateCertificateAuthority",
        "Effect" : "Allow",
        "Action" : [
            "acm-pca:GetCertificate",
            "acm-pca:GetCertificateAuthorityCertificate",
            "acm-pca:DescribeCertificateAuthority"
        ],
        "Resource" : "*",
        "Condition" : {
            "StringEquals" : {
                "aws:ResourceTag/AmazonECSManaged" : "true"
            }
        }
    },
    {
        "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
        "Effect" : "Allow",

```

```
"Action" : [
  "acm-pca:IssueCertificate"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/AmazonECSManaged" : "true",
    "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonECSInfrastructureRolePolicyForVolumes

Descrizione: fornisce l'accesso ad altre risorse AWS di servizio necessarie per gestire i volumi associati ai carichi di lavoro ECS per tuo conto.

AmazonECSInfrastructureRolePolicyForVolumes è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonECSInfrastructureRolePolicyForVolumes ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 gennaio 2024, 22:56 UTC
- Ora modificata: 10 gennaio 2024, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/AmazonECSManaged" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
            "aws:ResourceTag/AmazonECSManaged" : "true"
        }
    }
}

```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonECSServiceRolePolicy

Descrizione: policy per consentire ad Amazon ECS di gestire il cluster.

AmazonECSServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 ottobre 2017, 01:18 UTC
- Ora modificata: 04 dicembre 2023, 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonECSTaskExecutionRolePolicy

Descrizione: fornisce l'accesso ad altre risorse AWS di servizio necessarie per eseguire le attività di Amazon ECS

AmazonECSTaskExecutionRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonECSTaskExecutionRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 16 novembre 2017, 18:48 UTC
- Ora modificata: 16 novembre 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEFSCSIDriverPolicy

Descrizione: Fornisce l'accesso di gestione alle risorse EFS e l'accesso in lettura a EC2

AmazonEFSCSIDriverPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEFSCSIDriverPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 luglio 2023, 20:10 UTC
- Ora modificata: 25 luglio 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKS_CNI_Policy

Descrizione: questa policy fornisce al plugin Amazon VPC CNI (amazon-vpc-cni-k8s) le autorizzazioni necessarie per modificare la configurazione dell'indirizzo IP sui nodi di lavoro EKS. Questo set di autorizzazioni consente al CNI di elencare, descrivere e modificare le interfacce di rete elastiche per tuo conto. Ulteriori informazioni sul plugin AWS VPC CNI sono disponibili qui: <https://github.com/aws/8s-amazon-vpc-cni-k>

AmazonEKS_CNI_Policy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonEKS_CNI_Policy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2018, 21:07 UTC
- Ora modificata: 4 marzo 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSClusterPolicy

Descrizione: questa policy fornisce a Kubernetes le autorizzazioni necessarie per gestire le risorse per tuo conto. Kubernetes richiede Ec2: CreateTags autorizzazioni per inserire informazioni identificative sulle risorse EC2, tra cui, a titolo esemplificativo, istanze, gruppi di sicurezza e interfacce di rete elastiche.

AmazonEKSClusterPolicy [è una AWS politica gestita.](#)

Utilizzo di questa politica

Puoi collegarti AmazonEKSClusterPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2018, 21:06 UTC
- Ora modificata: 07 febbraio 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}

```

```
}  
  }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSCredentialsServiceRolePolicy

Descrizione: questa policy consente ad Amazon EKS di gestire AWS le risorse per il connettore EKS

AmazonEKSCredentialsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 04 settembre 2021, 20:31 UTC
- Ora modificata: 04 settembre 2021, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCredentialsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm>DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*:*:document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
```

```
"Action" : [
  "iam:PassRole"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "ssm.amazonaws.com"
    ]
  }
},
{
  "Sid" : "PutManagedEventRule",
  "Effect" : "Allow",
  "Action" : "events:PutRule",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "eks-connector.amazonaws.com",
      "events:source" : "aws.ssm"
    }
  }
},
{
  "Sid" : "PutManagedEventTarget",
  "Effect" : "Allow",
  "Action" : "events:PutTargets",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "eks-connector.amazonaws.com"
    }
  }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSFargatePodExecutionRolePolicy

Descrizione: fornisce l'accesso ad altre risorse AWS di servizio necessarie per eseguire i pod Amazon EKS su AWS Fargate

AmazonEKSFargatePodExecutionRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEKSFargatePodExecutionRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 novembre 2019, 04:34 UTC
- Ora modificata: 22 novembre 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ]
    }
  ]
}
```



```
    ],  
    "Resource" : "*"br/>  }br/>]br/>}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSFargateServiceRolePolicy

Descrizione: questa politica concede le autorizzazioni necessarie ad Amazon EKS per eseguire attività fargate

AmazonEKSFargateServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 22 novembre 2019, 04:36 UTC
- Ora modificata: 22 novembre 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSLocalOutpostClusterPolicy

Descrizione: questa policy fornisce le autorizzazioni alle istanze del piano di controllo del cluster locale EKS in esecuzione nel tuo account per gestire le risorse per tuo conto.

AmazonEKSLocalOutpostClusterPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonEKSLocalOutpostClusterPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 agosto 2022, 21:56 UTC
- Ora modificata: 17 ottobre 2022, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*:*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSLocalOutpostServiceRolePolicy

Descrizione: consente ad Amazon EKS Local di chiamare AWS i servizi per tuo conto.

AmazonEKSLocalOutpostServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 agosto 2022, 21:53 UTC
- Ora modificata: 24 ottobre 2022, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSServicePolicy

Descrizione: questa policy consente ad Amazon Elastic Container Service for Kubernetes di creare e gestire le risorse necessarie per gestire i cluster EKS.

AmazonEKSServicePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonEKSServicePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2018, 21:08 UTC
- Ora modificata: 27 maggio 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSServiceRolePolicy

Descrizione: è necessario un ruolo collegato ai servizi per consentire ad Amazon EKS di chiamare AWS i servizi per tuo conto.

AmazonEKSServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 febbraio 2020, 20:10 UTC
- Ora modificata: 27 maggio 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*:*:*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSVPCResourceController

Descrizione: Policy utilizzata da VPC Resource Controller per gestire ENI e IP per i nodi di lavoro.

AmazonEKSVPCResourceController è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEKSVPCResourceController ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 agosto 2020, 00:55 UTC
- Ora modificata: 12 agosto 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEKSWorkerNodePolicy

Descrizione: questa policy consente ai nodi di lavoro Amazon EKS di connettersi ai cluster Amazon EKS.

AmazonEKSWorkerNodePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEKSWorkerNodePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2018, 21:09 UTC
- Ora modificata: 27 novembre 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElastiCacheFullAccess

Descrizione: fornisce l'accesso completo ad Amazon ElastiCache tramite AWS Management Console.

AmazonElastiCacheFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElastiCacheFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC

- Ora modificata: 28 novembre 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : "elasticache:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/AWSServiceRoleForElastiCache",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticache.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpoints",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2::*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
},
{
  "Sid" : "TagVPCEndpointsOnCreation",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint",
      "aws:RequestTag/AmazonElastiCacheManaged" : "true"
    }
  }
},
{
  "Sid" : "AllowAccessToEc2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowAccessToKMS",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:ListKeys"
  ],
  "Resource" : "*"
}
```

```
    },
    {
      "Sid" : "AllowAccessToCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListLogDeliveryStreams",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "AllowAccessToOutposts",
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElastiCacheReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon ElastiCache tramite AWS Management Console.

AmazonElastiCacheReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElastiCacheReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticContainerRegistryPublicFullAccess

Descrizione: Fornisce accesso amministrativo alle risorse pubbliche di Amazon ECR

AmazonElasticContainerRegistryPublicFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticContainerRegistryPublicFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 17:25 UTC
- Ora modificata: 01 dicembre 2020, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticContainerRegistryPublicPowerUser

Descrizione: fornisce l'accesso completo agli archivi pubblici di Amazon ECR, ma non consente l'eliminazione degli archivi o la modifica delle policy.

AmazonElasticContainerRegistryPublicPowerUser [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticContainerRegistryPublicPowerUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 16:16 UTC
- Ora modificata: 01 dicembre 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticContainerRegistryPublicReadOnly

Descrizione: fornisce accesso in sola lettura ai repository pubblici di Amazon ECR.

AmazonElasticContainerRegistryPublicReadOnly è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonElasticContainerRegistryPublicReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 17:27 UTC
- Ora modificata: 01 dicembre 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticFileSystemClientFullAccess

Descrizione: fornisce l'accesso del client root a un file system Amazon EFS

AmazonElasticFileSystemClientFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticFileSystemClientFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 gennaio 2020, 16:27 UTC
- Ora modificata: 13 gennaio 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticFileSystemClientReadOnlyAccess

Descrizione: fornisce l'accesso client di sola lettura a un file system Amazon EFS

AmazonElasticFileSystemClientReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticFileSystemClientReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 gennaio 2020, 16:24 UTC

- Ora modificata: 13 gennaio 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticFileSystemClientReadWriteAccess

Descrizione: fornisce l'accesso client di lettura e scrittura a un file system Amazon EFS

AmazonElasticFileSystemClientReadWriteAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticFileSystemClientReadWriteAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 gennaio 2020, 16:21 UTC
- Ora modificata: 13 gennaio 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticFileSystemFullAccess

Descrizione: fornisce l'accesso completo ad Amazon EFS tramite AWS Management Console.

AmazonElasticFileSystemFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticFileSystemFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2015, 16:22 UTC
- Ora modificata: 28 novembre 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticFileSystemReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EFS tramite AWS Management Console.

AmazonElasticFileSystemReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticFileSystemReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2015, 16:25 UTC
- Ora modificata: 10 gennaio 2022, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticFileSystemServiceRolePolicy

Descrizione: consente ad Amazon Elastic File System di gestire AWS le risorse per tuo conto

AmazonElasticFileSystemServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 novembre 2019, 16:52 UTC
- Ora modificata: 10 gennaio 2022, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticFileSystemsUtils

Descrizione: consente ai clienti di utilizzare AWS Systems Manager per gestire automaticamente il pacchetto Amazon EFS utilities (amazon-efs-utils) sulle loro istanze EC2 e di utilizzarlo per CloudWatchLog ricevere notifiche di successo/errore del montaggio del file system EFS.

AmazonElasticFileSystemsUtils è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticFileSystemsUtils ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 settembre 2020, 15:16 UTC
- Ora modificata: 29 settembre 2020, 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticMapReduceEditorsRole

Descrizione: policy predefinita per il ruolo di servizio Amazon Elastic MapReduce Editors.

AmazonElasticMapReduceEditorsRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticMapReduceEditorsRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 16 novembre 2018, 21:55 UTC
- Ora modificata: 09 febbraio 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticMapReduceforAutoScalingRole

Descrizione: Amazon Elastic MapReduce for Auto Scaling. Ruolo per consentire ad Auto Scaling di aggiungere e rimuovere istanze dal cluster EMR.

AmazonElasticMapReduceforAutoScalingRole è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticMapReduceforAutoScalingRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 novembre 2016, 01:09 UTC
- Ora modificata: 18 novembre 2016, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticMapReduceforEC2Role

Descrizione: policy predefinita per il ruolo di servizio Amazon Elastic MapReduce for EC2.

AmazonElasticMapReduceforEC2Role è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticMapReduceforEC2Role ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 11 agosto 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticMapReduceFullAccess

Descrizione: questa politica si trova su un percorso obsoleto. Consulta la documentazione come guida: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/.html>. `emr-managed-iam-policies` Fornisce accesso completo ad Amazon Elastic MapReduce e ai servizi sottostanti che richiede, come EC2 e S3

AmazonElasticMapReduceFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticMapReduceFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 11 ottobre 2019, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticMapReducePlacementGroupPolicy

Descrizione: Politica per consentire a EMR di creare, descrivere ed eliminare i gruppi di collocamento EC2.

AmazonElasticMapReducePlacementGroupPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticMapReducePlacementGroupPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 settembre 2020, 00:37 UTC
- Ora modificata: 29 settembre 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticMapReduceReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Elastic MapReduce tramite AWS Management Console.

AmazonElasticMapReduceReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticMapReduceReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 29 luglio 2020, 23:14 UTC

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

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticMapReduceRole

Descrizione: questa politica si trova su un percorso obsoleto. Consulta la documentazione come guida: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/.html>. `emr-managed-iam-policies` Policy predefinita per il ruolo del MapReduce servizio Amazon Elastic.

AmazonElasticMapReduceRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticMapReduceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 24 giugno 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticsearchServiceRolePolicy

Descrizione: consenti ad Amazon Elasticsearch Service di accedere ad altri AWS servizi come le API di rete EC2 per tuo conto.

AmazonElasticsearchServiceRolePolicy [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 7 luglio 2017, 00:15 UTC
- Ora modificata: 23 ottobre 2023, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticTranscoder_FullAccess

Descrizione: concede agli utenti l'accesso completo a Elastic Transcoder e l'accesso ai servizi associati necessari per la funzionalità completa di Elastic Transcoder.

AmazonElasticTranscoder_FullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonElasticTranscoder_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 aprile 2018, 18:59 UTC

- Ora modificata: 10 giugno 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
          ]
        }
      }
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticTranscoder_JobsSubmitter

Descrizione: concede agli utenti il permesso di modificare le preimpostazioni, inviare lavori e visualizzare le impostazioni di Elastic Transcoder. Questa politica concede inoltre un accesso in sola lettura ad alcuni altri servizi necessari per utilizzare la console Elastic Transcode, tra cui S3, IAM e SNS.

AmazonElasticTranscoder_JobsSubmitter [è una politica AWS gestita.](#)

Utilizzo di questa politica

Puoi collegarti AmazonElasticTranscoder_JobsSubmitter ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 giugno 2018, 21:12 UTC
- Ora modificata: 10 giugno 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticTranscoder_ReadOnlyAccess

Descrizione: concede agli utenti l'accesso in sola lettura a Elastic Transcoder e l'accesso agli elenchi ai servizi correlati.

AmazonElasticTranscoder_ReadOnlyAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonElasticTranscoder_ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 07 giugno 2018, 21:09 UTC
- Ora modificata: 10 giugno 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonElasticTranscoderRole

Descrizione: policy predefinita per il ruolo del servizio Amazon Elastic Transcoder.

AmazonElasticTranscoderRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonElasticTranscoderRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 13 giugno 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEMRCleanupPolicy

Descrizione: consente le azioni richieste da EMR per terminare ed eliminare le risorse AWS EC2 se il ruolo del servizio EMR ha perso tale capacità.

AmazonEMRCleanupPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 settembre 2017, 23:54 UTC
- Ora modificata: 29 settembre 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  ]
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEMRContainersServiceRolePolicy

Descrizione: consente l'accesso ad altre risorse di AWS servizio necessarie per eseguire Amazon EMR

AmazonEMRContainersServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 09 dicembre 2020, 00:38 UTC
- Ora modificata: 10 marzo 2023, 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
  ]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEMRFullAccessPolicy_v2

Descrizione: Fornisce accesso completo ad Amazon EMR

AmazonEMRFullAccessPolicy_v2 è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEMRFullAccessPolicy_v2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 marzo 2021, 01:50 UTC
- Ora modificata: 28 luglio 2023, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEMRReadOnlyAccessPolicy_v2

Descrizione: fornisce accesso in sola lettura ad Amazon EMR e alle metriche associate CloudWatch .

AmazonEMRReadOnlyAccessPolicy_v2 è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEMRReadOnlyAccessPolicy_v2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 marzo 2021, 01:39 UTC
- Ora modificata: 02 agosto 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEMRServerlessServiceRolePolicy

Descrizione: consente l'accesso ad altre risorse AWS di servizio necessarie per eseguire Amazon EMRServerless

AmazonEMRServerlessServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 maggio 2022, 23:15 UTC
- Ora modificata: 25 gennaio 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
          ]
        }
      }
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEMRServicePolicy_v2

Descrizione: questa policy viene utilizzata per il ruolo del servizio Amazon EMR e NON deve essere utilizzata per altri utenti o ruoli IAM nel tuo account. La politica concede le autorizzazioni per creare e gestire le risorse associate all'EMR e ai servizi correlati necessari per il funzionamento del cluster EMR.

AmazonEMRServicePolicy_v2 [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonEMRServicePolicy_v2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 marzo 2021, 01:11 UTC
- Ora modificata: 2 maggio 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CreateInTaggedNetwork",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface",
      "ec2:RunInstances",
      "ec2:CreateFleet",
      "ec2:CreateLaunchTemplate",
      "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
      }
    }
  },
  {
    "Sid" : "CreateWithEMRTaggedLaunchTemplate",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateFleet",
      "ec2:RunInstances",
      "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
      }
    }
  },
  {
    "Sid" : "CreateEMRTaggedLaunchTemplate",
    "Effect" : "Allow",
    "Action" : "ec2:CreateLaunchTemplate",
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "StringEquals" : {

```



```

        "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
}
},
{
    "Sid" : "CreateEMRTaggedInstancesAndVolumes",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
},
{
    "Sid" : "ResourcesToLaunchEC2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
    ]
},
{
    "Sid" : "ManageEMRTaggedResources",
    "Effect" : "Allow",

```

```

    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:DeleteLaunchTemplate",
      "ec2:DeleteNetworkInterface",
      "ec2:ModifyInstanceAttribute",
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
      }
    }
  },
  {
    "Sid" : "ManageTagsOnEMRTaggedResources",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2:DeleteTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
      }
    }
  },
  {
    "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringEquals" : {

```

```

        "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
}
},
{
    "Sid" : "TagOnCreateTaggedEMRResources",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ec2:CreateAction" : [
                "RunInstances",
                "CreateFleet",
                "CreateLaunchTemplate",
                "CreateNetworkInterface"
            ]
        }
    }
},
{
    "Sid" : "TagPlacementGroups",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
    ]
},
{
    "Sid" : "ListActionsForEC2Resources",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",

```

```

        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
},
{
    "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
    ],
    "Condition" : {

```

```
        "StringEquals" : {
            "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    },
    {
        "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
        "Effect" : "Allow",
        "Action" : [
            "ec2:CreateTags"
        ],
        "Resource" : "arn:aws:ec2:*:*:security-group/*",
        "Condition" : {
            "StringEquals" : {
                "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
                "ec2:CreateAction" : "CreateSecurityGroup"
            }
        }
    },
    {
        "Sid" : "ManageSecurityGroups",
        "Effect" : "Allow",
        "Action" : [
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress"
        ],
        "Resource" : "*",
        "Condition" : {
            "StringEquals" : {
                "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
            }
        }
    },
    {
        "Sid" : "CreateEMRPlacementGroups",
        "Effect" : "Allow",
        "Action" : [
            "ec2:CreatePlacementGroup"
        ],
        "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
```

```

    "Sid" : "DeletePlacementGroups",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeletePlacementGroup"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AutoScaling",
    "Effect" : "Allow",
    "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ResourceGroupsForCapacityReservations",
    "Effect" : "Allow",
    "Action" : [
        "resource-groups:ListGroupResources"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AutoScalingCloudWatch",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
},
{
    "Sid" : "PassRoleForAutoScaling",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
    "Condition" : {

```

```
    "StringLike" : {
      "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
    }
  },
  {
    "Sid" : "PassRoleForEC2",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ec2.amazonaws.com*"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonESCognitoAccess

Descrizione: fornisce un accesso limitato al servizio di configurazione Amazon Cognito.

AmazonESCognitoAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonESCognitoAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 28 febbraio 2018, 22:29 UTC
- Ora modificata: 20 dicembre 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"  
]  
}  
}  
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonESFullAccess

Descrizione: fornisce l'accesso completo al servizio di configurazione Amazon ES.

AmazonESFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonESFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 ottobre 2015, 19:14 UTC
- Ora modificata: 1 ottobre 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonESReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio di configurazione Amazon ES.

AmazonESReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonESReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 1 ottobre 2015, 19:18 UTC
- Ora modificata: 03 ottobre 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

Descrizione: consente di accedere EventBridge alle risorse di Secret Manager per tuo conto.

AmazonEventBridgeApiDestinationsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 11 febbraio 2021, 20:52 UTC
- Ora modificata: 11 febbraio 2021, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgeFullAccess

Descrizione: fornisce l'accesso completo ad Amazon EventBridge.

AmazonEventBridgeFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 luglio 2019, 14:08 UTC
- Ora modificata: 01 dicembre 2022, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgePipesFullAccess

Descrizione: fornisce l'accesso completo ad Amazon EventBridge Pipes.

AmazonEventBridgePipesFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgePipesFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2022, 17:03 UTC
- Ora modificata: 01 dicembre 2022, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgePipesOperatorAccess

Descrizione: fornisce l'accesso in sola lettura e all'operatore (possibilità di interrompere e avviare Pipes) ad Amazon EventBridge Pipes.

AmazonEventBridgePipesOperatorAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgePipesOperatorAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2022, 17:04 UTC
- Ora modificata: 01 dicembre 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgePipesReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EventBridge Pipes.

AmazonEventBridgePipesReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgePipesReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2022, 17:04 UTC
- Ora modificata: 01 dicembre 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgeReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EventBridge.

AmazonEventBridgeReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgeReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 luglio 2019, 13:59 UTC
- Ora modificata: 01 dicembre 2022, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgeSchedulerFullAccess

Descrizione: la politica AmazonEventBridgeSchedulerFullAccess gestita concede le autorizzazioni per utilizzare tutte le azioni di EventBridge Scheduler per le pianificazioni e i gruppi di pianificazioni.

AmazonEventBridgeSchedulerFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgeSchedulerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2022, 18:37 UTC
- Ora modificata: 10 novembre 2022, 18:37 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgeSchedulerReadOnlyAccess

Descrizione: la politica AmazonEventBridgeSchedulerReadOnlyAccess gestita concede autorizzazioni di sola lettura per visualizzare i dettagli sulle pianificazioni e sui gruppi di pianificazioni

AmazonEventBridgeSchedulerReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgeSchedulerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2022, 18:50 UTC
- Ora modificata: 10 novembre 2022, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ]
    }
  ]
}
```



```
    ],  
    "Resource" : "*"br/>  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgeSchemasFullAccess

Descrizione: fornisce l'accesso completo ad Amazon EventBridge Schemas.

AmazonEventBridgeSchemasFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgeSchemasFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2019, 23:12 UTC
- Ora modificata: 28 novembre 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgeSchemasReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EventBridge Schemas.

AmazonEventBridgeSchemasReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonEventBridgeSchemasReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2019, 23:05 UTC
- Ora modificata: 01 maggio 2020, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonEventBridgeSchemasServiceRolePolicy

Descrizione: concede le autorizzazioni per le Managed Rules create dagli schemi Amazon EventBridge .

AmazonEventBridgeSchemasServiceRolePolicy [è una politica gestita AWS](#) .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi

- Ora di creazione: 27 novembre 2019, 01:10 UTC
- Ora modificata: 27 novembre 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFISServiceRolePolicy

Descrizione: Politica per consentire alla AWS FIS di gestire il monitoraggio e la selezione delle risorse per gli esperimenti.

AmazonFISServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 dicembre 2020, 21:18 UTC
- Ora modificata: 25 ottobre 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonForecastFullAccess

Descrizione: Fornisce accesso a tutte le azioni per Amazon Forecast

AmazonForecastFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonForecastFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2019, 01:52 UTC
- Ora modificata: 18 gennaio 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFraudDetectorFullAccessPolicy

Descrizione: Fornisce accesso a tutte le azioni per Amazon Fraud Detector

AmazonFraudDetectorFullAccessPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonFraudDetectorFullAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 22:46 UTC
- Ora modificata: 03 dicembre 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFreeRTOSFullAccess

Descrizione: Policy di accesso completo per Amazon FreeRTOS

AmazonFreeRTOSFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonFreeRTOSFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 15:32 UTC
- Ora modificata: 29 novembre 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFreeRTOSOTAUpdate

Descrizione: consente all'utente di accedere ad Amazon FreeRTOS OTA Update

AmazonFreeRTOSOTAUpdate è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonFreeRTOSOTAUpdate ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 agosto 2018, 22:43 UTC
- Ora modificata: 18 dicembre 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::afr-ota*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "signer:StartSigningJob",
        "signer:DescribeSigningJob",
        "signer:GetSigningProfile",
        "signer:PutSigningProfile"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "iot>DeleteJob",
        "iot:DescribeJob"
    ],
    "Resource" : "arn:aws:iot:*:*:job/AFR_OTA*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "iot>DeleteStream"
    ],
    "Resource" : "arn:aws:iot:*:*:stream/AFR_OTA*"
},
{
```

```
"Effect" : "Allow",
"Action" : [
    "iot:CreateStream",
    "iot:CreateJob"
],
"Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFSxConsoleFullAccess

Descrizione: fornisce l'accesso completo ad Amazon FSx e l'accesso ai AWS servizi correlati tramite AWS Management Console

AmazonFSxConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonFSxConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 16:36 UTC
- Ora modificata: 10 gennaio 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
    }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFSxConsoleReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon FSx e accesso ai AWS servizi correlati tramite. AWS Management Console

AmazonFSxConsoleReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonFSxConsoleReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 28 novembre 2018, 16:35 UTC
- Ora modificata: 10 gennaio 2024, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFSxFullAccess

Descrizione: fornisce l'accesso completo ad Amazon FSx e l'accesso ai servizi correlati AWS .

AmazonFSxFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonFSxFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 16:34 UTC
- Ora modificata: 10 gennaio 2024, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
                "ram.amazonaws.com"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFSxReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon FSx.

AmazonFSxReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonFSxReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 16:33 UTC
- Ora modificata: 28 novembre 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonFSxServiceRolePolicy

Descrizione: consente ad Amazon FSx di gestire AWS le risorse per tuo conto

AmazonFSxServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 28 novembre 2018, 10:38 UTC
- Ora modificata: 10 gennaio 2024, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGlacierFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Glacier tramite. AWS Management Console

AmazonGlacierFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonGlacierFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGlacierReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Glacier tramite AWS Management Console

AmazonGlacierReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonGlacierReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 5 maggio 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGrafanaAthenaAccess

Descrizione: questa politica consente l'accesso ad Amazon Athena e alle dipendenze necessarie per consentire l'esecuzione di query e la scrittura dei risultati su s3 dal plug-in Amazon Athena in Amazon Grafana.

AmazonGrafanaAthenaAccess è una [politica](#) gestita AWS.

Utilizzo di questa politica

Puoi collegarti AmazonGrafanaAthenaAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 novembre 2021, 17:11 UTC
- Ora modificata: 22 novembre 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
    ]
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGrafanaCloudWatchAccess

Descrizione: questa politica garantisce l'accesso ad Amazon CloudWatch e alle dipendenze necessarie per l'uso CloudWatch come origine dati all'interno di Amazon Managed Grafana.

AmazonGrafanaCloudWatchAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonGrafanaCloudWatchAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 marzo 2023, 22:41 UTC
- Ora modificata: 24 marzo 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGrafanaRedshiftAccess

Descrizione: questa policy garantisce l'accesso mirato ad Amazon Redshift e alle dipendenze necessarie per utilizzare il plug-in Amazon Redshift in Amazon Grafana.

AmazonGrafanaRedshiftAccess [AWS è una politica](#) gestita.

Utilizzo di questa politica

Puoi collegarti AmazonGrafanaRedshiftAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 novembre 2021, 23:15 UTC
- Ora modificata: 26 novembre 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGrafanaServiceLinkedRolePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate da Amazon Grafana.

AmazonGrafanaServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 08 novembre 2022, 23:10 UTC
- Ora modificata: 08 novembre 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGuardDutyFullAccess

Descrizione: fornisce l'accesso completo all'uso di Amazon GuardDuty.

AmazonGuardDutyFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonGuardDutyFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2017, 22:31 UTC
- Ora modificata: 10 giugno 2024, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",

```

```

        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IamGetRoleSid1",
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
  },
  {
    "Sid" : "AllowPassRoleToMalwareProtectionPlan",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "malware-protection-plan.guardduty.amazonaws.com"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Descrizione: la protezione GuardDuty da malware utilizza il ruolo collegato al servizio (SLR) denominato. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Questo ruolo collegato al servizio consente alla protezione GuardDuty da malware di eseguire scansioni senza agente

per rilevare il malware. Consente di GuardDuty creare istantanee nell'account e condividerle con l'account del servizio per individuare eventuali malware. GuardDuty Valuta queste istantanee condivise e include i metadati delle istanze EC2 recuperati nei risultati di Malware Protection. GuardDuty Il ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio si fida del servizio `malware-protection.guardduty.amazonaws.com` per l'assunzione del ruolo.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` è [AWS una](#) politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 luglio 2022, 19:06 UTC
- Ora modificata: 25 gennaio 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/guarddduty/*"
  },
  {
    "Sid" : "GuardDutyLogStreamPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/guarddduty/*: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"
      }
    }
  }
}

```

```
}  
  }  
  ]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGuardDutyReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle GuardDuty risorse Amazon

AmazonGuardDutyReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonGuardDutyReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2017, 22:29 UTC
- Ora modificata: 16 novembre 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonGuardDutyServiceRolePolicy

Descrizione: Abilita l'accesso alle AWS risorse utilizzate o gestite da Amazon Guard Duty

AmazonGuardDutyServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 28 novembre 2017, 20:12 UTC
- Ora modificata: 27 marzo 2024, 00:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
}

```



```

    ]
  }
}
},
{
  "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeAssociation",
    "ssm>DeleteAssociation",
    "ssm:UpdateAssociation",
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce"
  ],
  "Resource" : "arn:aws:ssm:*:*:association/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/GuardDutyManaged" : "true"
    }
  }
},
{
  "Sid" : "SsmAddTagsToResourcePermission",
  "Effect" : "Allow",
  "Action" : [
    "ssm:AddTagsToResource"
  ],
  "Resource" : "arn:aws:ssm:*:*:association/*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "GuardDutyManaged"
      ]
    },
    "StringEquals" : {
      "aws:ResourceTag/GuardDutyManaged" : "true"
    }
  }
},
{
  "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",

```

```
    "ssm:UpdateAssociation"
  ],
  "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
},
{
  "Sid" : "SsmSendCommandPermission",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
  ]
},
{
  "Sid" : "SsmGetCommandStatus",
  "Effect" : "Allow",
  "Action" : "ssm:GetCommandInvocation",
  "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHealthLakeFullAccess

Descrizione: fornisce l'accesso completo al HealthLake servizio Amazon.

AmazonHealthLakeFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonHealthLakeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 17 febbraio 2021, 01:07 UTC
- Ora modificata: 17 febbraio 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHealthLakeReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al HealthLake servizio Amazon.

AmazonHealthLakeReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonHealthLakeReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 02:43 UTC
- Ora modificata: 17 febbraio 2021, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHoneycodeFullAccess

Descrizione: fornisce l'accesso completo a Honeycode tramite AWS Management Console e l'SDK.

AmazonHoneycodeFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonHoneycodeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:28 UTC

- Ora modificata: 24 giugno 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHoneycodeReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Honeycode tramite AWS Management Console e l'SDK.

AmazonHoneycodeReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonHoneycodeReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 01 dicembre 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHoneycodeServiceRolePolicy

Descrizione: è necessario un ruolo collegato al servizio per consentire ad Amazon Honeycode di accedere alle tue risorse.

AmazonHoneycodeServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 novembre 2020, 18:03 UTC
- Ora modificata: 18 novembre 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHoneycodeTeamAssociationFullAccess

Descrizione: fornisce l'accesso completo a Honeycode Team Association tramite AWS Management Console e l'SDK.

AmazonHoneycodeTeamAssociationFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonHoneycodeTeamAssociationFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 24 giugno 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Honeycode Team Association tramite AWS Management Console e l'SDK.

AmazonHoneycodeTeamAssociationReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonHoneycodeTeamAssociationReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:27 UTC
- Ora modificata: 24 giugno 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHoneycodeWorkbookFullAccess

Descrizione: fornisce l'accesso completo a Honeycode Workbook tramite AWS Management Console e l'SDK.

AmazonHoneycodeWorkbookFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonHoneycodeWorkbookFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 01 dicembre 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonHoneycodeWorkbookReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Honeycode Workbook tramite AWS Management Console e l'SDK.

AmazonHoneycodeWorkbookReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonHoneycodeWorkbookReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 01 dicembre 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonInspector2AgentlessServiceRolePolicy

Descrizione: concede ad Amazon Inspector l'accesso alle valutazioni di sicurezza necessarie Servizi AWS per eseguire valutazioni di sicurezza senza agenti

AmazonInspector2AgentlessServiceRolePolicy è [una](#) politica gestita AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 novembre 2023, 15:18 UTC
- Ora modificata: 20 novembre 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonInspector2FullAccess

Descrizione: fornisce l'accesso completo ad Amazon Inspector e l'accesso ad altri servizi correlati, come le organizzazioni.

AmazonInspector2FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonInspector2FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 19:10 UTC
- Ora modificata: 25 aprile 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
```

```
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonInspector2ManagedCisPolicy

Descrizione: si tratta di una politica gestita che il cliente deve associare ai propri ruoli per comunicare con il servizio di ispezione per le scansioni CIS

AmazonInspector2ManagedCisPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonInspector2ManagedCisPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 gennaio 2024, 16:31 UTC
- Ora modificata: 24 gennaio 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonInspector2ReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio Amazon inspector2 e ai servizi di supporto pertinenti

AmazonInspector2ReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonInspector2ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 gennaio 2022, 14:45 UTC
- Ora modificata: 22 settembre 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonInspector2ServiceRolePolicy

Descrizione: concede ad Amazon Inspector l'accesso ai dati necessari Servizi AWS per eseguire le valutazioni di sicurezza

AmazonInspector2ServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 novembre 2021, 20:27 UTC
- Ora modificata: 22 gennaio 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonInspectorFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Inspector.

AmazonInspectorFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonInspectorFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 ottobre 2015, 17:08 UTC
- Ora modificata: 21 dicembre 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonInspectorReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Inspector.

AmazonInspectorReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonInspectorReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 ottobre 2015, 17:08 UTC
- Ora modificata: 1 ottobre 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonInspectorServiceRolePolicy

Descrizione: concede ad Amazon Inspector l'accesso ai dati necessari Servizi AWS per eseguire le valutazioni di sicurezza

AmazonInspectorServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 novembre 2017, 15:48 UTC
- Ora modificata: 11 settembre 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKendraFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Kendra tramite AWS Management Console

AmazonKendraFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKendraFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 16:15 UTC
- Ora modificata: 03 dicembre 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKendraReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon Kendra tramite AWS Management Console.

AmazonKendraReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKendraReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 03 dicembre 2019, 16:13 UTC
- Ora modificata: 27 maggio 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKeyspacesFullAccess

Descrizione: Fornisci l'accesso completo ad Amazon Keyspaces

AmazonKeyspacesFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKeyspacesFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2020, 17:06 UTC
- Ora modificata: 03 ottobre 2023, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKeyspacesReadOnlyAccess

Descrizione: Fornisci accesso in sola lettura ad Amazon Keyspaces

AmazonKeyspacesReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKeyspacesReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 23 aprile 2020, 17:07 UTC
- Ora modificata: 07 luglio 2022, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKeyspacesReadOnlyAccess_v2

Descrizione: Fornisci accesso in sola lettura ad Amazon Keyspaces e ai servizi correlati AWS .

AmazonKeyspacesReadOnlyAccess_v2 è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKeyspacesReadOnlyAccess_v2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 settembre 2023, 17:01 UTC
- Ora modificata: 12 settembre 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKinesisAnalyticsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Kinesis Analytics tramite AWS Management Console.

AmazonKinesisAnalyticsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKinesisAnalyticsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 settembre 2016, 19:01 UTC
- Ora modificata: 21 settembre 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}
]

```



```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKinesisAnalyticsReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Kinesis Analytics tramite. AWS Management Console

AmazonKinesisAnalyticsReadOnly è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonKinesisAnalyticsReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 settembre 2016, 18:16 UTC
- Ora modificata: 21 settembre 2016, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKinesisFirehoseFullAccess

Descrizione: fornisce l'accesso completo a tutti i flussi di distribuzione di Amazon Kinesis Firehose.

AmazonKinesisFirehoseFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonKinesisFirehoseFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 ottobre 2015, 18:45 UTC
- Ora modificata: 7 ottobre 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKinesisFirehoseReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutti gli Amazon Kinesis Firehose Delivery Streams.

AmazonKinesisFirehoseReadOnlyAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonKinesisFirehoseReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 7 ottobre 2015, 18:43 UTC
- Ora modificata: 7 ottobre 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKinesisFullAccess

Descrizione: fornisce l'accesso completo a tutti gli stream tramite. AWS Management Console

AmazonKinesisFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKinesisFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKinesisReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutti gli stream tramite AWS Management Console

AmazonKinesisReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKinesisReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```

```
        "kinesis:List*",
        "kinesis:Describe*"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKinesisVideoStreamsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Kinesis Video AWS Management Console Streams tramite.

AmazonKinesisVideoStreamsFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKinesisVideoStreamsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2017, 23:27 UTC
- Ora modificata: 01 dicembre 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonKinesisVideoStreamsReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura a AWS Kinesis Video AWS Management Console Streams tramite.

AmazonKinesisVideoStreamsReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonKinesisVideoStreamsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2017, 23:14 UTC

- Ora modificata: 01 dicembre 2017, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLaunchWizard_Fullaccess

Descrizione: accesso completo alla procedura guidata di AWS avvio e ad altri servizi richiesti.

AmazonLaunchWizard_Fullaccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonLaunchWizard_Fullaccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 agosto 2020, 17:47 UTC
- Ora modificata: 22 febbraio 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLaunchWizardFullAccessV2

Descrizione: accesso completo alla procedura guidata di AWS avvio e ad altri servizi richiesti.

AmazonLaunchWizardFullAccessV2 è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonLaunchWizardFullAccessV2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 settembre 2023, 17:14 UTC
- Ora modificata: 01 settembre 2023, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLexChannelsAccess

Descrizione: Questa politica consente ai clienti di chiamare Lex runtime dai canali

AmazonLexChannelsAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 gennaio 2021, 20:12 UTC
- Ora modificata: 13 gennaio 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Action" : [
      "lex:ListBots"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLexFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Lex tramite AWS Management Console. Fornisce inoltre l'accesso per creare Lex Service Linked Roles e concedere le autorizzazioni Lex per richiamare un set limitato di funzioni Lambda.

AmazonLexFullAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonLexFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 aprile 2017, 23:20 UTC
- Ora modificata: 16 aprile 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
```

```

        "lambda:Principal" : "lex.amazonaws.com"
    }
}
},
{
    "Sid" : "AmazonLexFullAccessStatement3",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ]
},
{
    "Sid" : "AmazonLexFullAccessStatement4",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "lex.amazonaws.com"
        }
    }
},
{
    "Sid" : "AmazonLexFullAccessStatement5",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ]
}

```

```

    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
    }
},
{
    "Sid" : "AmazonLexFullAccessStatement6",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
    }
},
{
    "Sid" : "AmazonLexFullAccessStatement7",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
    }
},
{

```

```

    "Sid" : "AmazonLexFullAccessStatement8",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "replication.lexv2.amazonaws.com"
        }
    }
},
{
    "Sid" : "AmazonLexFullAccessStatement9",
    "Effect" : "Allow",
    "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ]
},
{
    "Sid" : "AmazonLexFullAccessStatement10",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
    ]
}

```



```

    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lex.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement11",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lexv2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement12",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "channels.lexv2.amazonaws.com"
        ]
      }
    }
  }
}

```

```
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLexReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Lex.

AmazonLexReadOnly è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonLexReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 aprile 2017, 23:13 UTC
- Ora modificata: 13 maggio 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexReadOnlyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",

```

```

    "lex:GetUtterancesView",
    "lex:DescribeBot",
    "lex:DescribeBotAlias",
    "lex:DescribeBotChannel",
    "lex:DescribeBotLocale",
    "lex:DescribeBotRecommendation",
    "lex:DescribeBotReplica",
    "lex:DescribeBotVersion",
    "lex:DescribeExport",
    "lex:DescribeImport",
    "lex:DescribeIntent",
    "lex:DescribeResourcePolicy",
    "lex:DescribeSlot",
    "lex:DescribeSlotType",
    "lex:ListBots",
    "lex:ListBotLocales",
    "lex:ListBotAliases",
    "lex:ListBotAliasReplicas",
    "lex:ListBotChannels",
    "lex:ListBotRecommendations",
    "lex:ListBotReplicas",
    "lex:ListBotVersions",
    "lex:ListBotVersionReplicas",
    "lex:ListBuiltInIntents",
    "lex:ListBuiltInSlotTypes",
    "lex:ListExports",
    "lex:ListImports",
    "lex:ListIntents",
    "lex:ListRecommendedIntents",
    "lex:ListSlots",
    "lex:ListSlotTypes",
    "lex:ListTagsForResource",
    "lex:SearchAssociatedTranscripts",
    "lex:ListCustomVocabularyItems"
  ],
  "Resource" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLexReplicationPolicy

Descrizione: consente ad Amazon Lex di replicare le risorse Lex tra le regioni per tuo conto.

AmazonLexReplicationPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 31 gennaio 2024, 23:29 UTC
- Ora modificata: 8 marzo 2024, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLexRunBotsOnly

Descrizione: fornisce l'accesso alle API conversazionali di Amazon Lex.

AmazonLexRunBotsOnly [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonLexRunBotsOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 aprile 2017, 23:06 UTC
- Ora modificata: 18 agosto 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLexV2BotPolicy

Descrizione: Fornisce ai bot Lex V2 l'accesso per chiamare altri AWS servizi per tuo conto.

AmazonLexV2BotPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 gennaio 2021, 20:10 UTC
- Ora modificata: 13 gennaio 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLookoutEquipmentFullAccess

Descrizione: Fornisce accesso completo alle operazioni di Amazon Lookout for Equipment

AmazonLookoutEquipmentFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonLookoutEquipmentFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 8 aprile 2021, 15:52 UTC
- Ora modificata: 24 novembre 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLookoutEquipmentReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura ad Amazon Lookout for Equipments

AmazonLookoutEquipmentReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonLookoutEquipmentReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 maggio 2021, 16:47 UTC
- Ora modificata: 10 novembre 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLookoutMetricsFullAccess

Descrizione: Fornisce accesso a tutte le azioni per Amazon Lookout for Metrics

AmazonLookoutMetricsFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonLookoutMetricsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 07 maggio 2021, 00:43 UTC
- Ora modificata: 07 maggio 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLookoutMetricsReadOnlyAccess

Descrizione: dà accesso a tutte le azioni di sola lettura per Amazon Lookout for Metrics

AmazonLookoutMetricsReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonLookoutMetricsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 07 maggio 2021, 00:43 UTC
- Ora modificata: 04 gennaio 2022, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLookoutVisionConsoleFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Lookout for Vision e l'accesso mirato al servizio richiesto e alle dipendenze della console.

AmazonLookoutVisionConsoleFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonLookoutVisionConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 11 maggio 2021, 19:37 UTC
- Ora modificata: 11 maggio 2021, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLookoutVisionConsoleReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Lookout for Vision e accesso mirato al servizio richiesto e alle dipendenze della console.

AmazonLookoutVisionConsoleReadOnlyAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonLookoutVisionConsoleReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 11 maggio 2021, 19:32 UTC
- Ora modificata: 09 dicembre 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLookoutVisionFullAccess

Descrizione: fornisce accesso completo ad Amazon Lookout for Vision e accesso mirato alle dipendenze richieste.

AmazonLookoutVisionFullAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonLookoutVisionFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2021, 19:24 UTC
- Ora modificata: 11 maggio 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonLookoutVisionReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Lookout for Vision e accesso mirato alle dipendenze richieste.

AmazonLookoutVisionReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonLookoutVisionReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2021, 19:11 UTC
- Ora modificata: 09 dicembre 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMachineLearningBatchPredictionsAccess

Descrizione: concede agli utenti l'autorizzazione a richiedere previsioni in batch su Amazon Machine Learning.

AmazonMachineLearningBatchPredictionsAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMachineLearningBatchPredictionsAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:12 UTC
- Ora modificata: 9 aprile 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "*"br/>  }br/>]br/>}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMachineLearningCreateOnlyAccess

Descrizione: fornisce accesso diretto a risorse Amazon Machine Learning non predittive.

AmazonMachineLearningCreateOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMachineLearningCreateOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:18 UTC
- Ora modificata: 29 giugno 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMachineLearningFullAccess

Descrizione: fornisce l'accesso completo alle risorse di Amazon Machine Learning.

AmazonMachineLearningFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMachineLearningFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 9 aprile 2015, 17:25 UTC
- Ora modificata: 9 aprile 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Descrizione: concede agli utenti l'autorizzazione a creare ed eliminare l'endpoint in tempo reale per i modelli di Amazon Machine Learning.

AmazonMachineLearningManageRealTimeEndpointOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMachineLearningManageRealTimeEndpointOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:32 UTC
- Ora modificata: 9 aprile 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMachineLearningReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle risorse di Amazon Machine Learning.

AmazonMachineLearningReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMachineLearningReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:40 UTC
- Ora modificata: 9 aprile 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

Descrizione: concede agli utenti l'autorizzazione a richiedere previsioni in tempo reale di Amazon Machine Learning.

AmazonMachineLearningRealTimePredictionOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMachineLearningRealTimePredictionOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:44 UTC
- Ora modificata: 9 aprile 2015, 17:44 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

Descrizione: consente al Machine Learning di configurare e utilizzare i cluster Redshift e le location di staging S3 per Redshift Data Source.

AmazonMachineLearningRoleforRedshiftDataSourceV3 [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonMachineLearningRoleforRedshiftDataSourceV3 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 giugno 2020, 18:00 UTC
- Ora modificata: 24 giugno 2020, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMacieFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Macie.

AmazonMacieFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMacieFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 14 agosto 2017, 14:54 UTC
- Ora modificata: 01 luglio 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMacieHandshakeRole

Descrizione: concede l'autorizzazione a creare il ruolo collegato al servizio di Amazon Macie.

AmazonMacieHandshakeRole è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonMacieHandshakeRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 giugno 2018, 15:46 UTC
- Ora modificata: 28 giugno 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "iam:AWSServiceName" : "macie.amazonaws.com"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMacieReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon Macie.

AmazonMacieReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMacieReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 giugno 2023, 21:50 UTC
- Ora modificata: 15 giugno 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMacieServiceRole

Descrizione: concede a Macie l'accesso in sola lettura alle dipendenze delle risorse del tuo account per consentire l'analisi dei dati.

AmazonMacieServiceRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonMacieServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 14:53 UTC
- Ora modificata: 14 agosto 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMacieServiceRolePolicy

Descrizione: ruolo collegato al servizio per Amazon Macie

AmazonMacieServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 giugno 2018, 22:17 UTC
- Ora modificata: 19 maggio 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
    ]
  }

```

```
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonManagedBlockchainConsoleFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon Managed Blockchain tramite AWS Management Console

AmazonManagedBlockchainConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonManagedBlockchainConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 aprile 2019, 21:23 UTC
- Ora modificata: 29 aprile 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonManagedBlockchainFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Managed Blockchain.

AmazonManagedBlockchainFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonManagedBlockchainFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 aprile 2019, 21:39 UTC

- Ora modificata: 29 aprile 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonManagedBlockchainReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Managed Blockchain.

AmazonManagedBlockchainReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonManagedBlockchainReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 aprile 2019, 18:17 UTC
- Ora modificata: 30 aprile 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonManagedBlockchainServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon Managed Blockchain

AmazonManagedBlockchainServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 gennaio 2020, 19:51 UTC
- Ora modificata: 17 gennaio 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMCSFullAccess

Descrizione: Fornisci l'accesso completo al servizio Amazon Managed Apache Cassandra

AmazonMCSFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMCSFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 13:45 UTC
- Ora modificata: 17 aprile 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMCSReadOnlyAccess

Descrizione: Fornisci accesso in sola lettura al servizio Amazon Managed Apache Cassandra

AmazonMCSReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonMCSReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 13:46 UTC
- Ora modificata: 17 aprile 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMechanicalTurkFullAccess

Descrizione: fornisce l'accesso completo a tutte le API in Amazon Mechanical Turk.

AmazonMechanicalTurkFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMechanicalTurkFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2015, 19:08 UTC
- Ora modificata: 11 dicembre 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMechanicalTurkReadOnly

Descrizione: fornisce l'accesso alle API di sola lettura in Amazon Mechanical Turk.

AmazonMechanicalTurkReadOnly è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMechanicalTurkReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2015, 19:08 UTC
- Ora modificata: 25 settembre 2019, 21:06 UTC

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

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMemoryDBFullAccess

Descrizione: fornisce l'accesso completo ad Amazon MemoryDB tramite AWS Management Console

AmazonMemoryDBFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMemoryDBFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 08 ottobre 2021, 19:24 UTC
- Ora modificata: 08 ottobre 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

```
}  
  }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMemoryDBReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon MemoryDB tramite AWS Management Console

AmazonMemoryDBReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMemoryDBReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 8 ottobre 2021, 19:27 UTC
- Ora modificata: 08 ottobre 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMobileAnalyticsFinancialReportAccess

Descrizione: fornisce accesso in sola lettura a tutti i report, inclusi i dati finanziari per tutte le risorse dell'applicazione.

AmazonMobileAnalyticsFinancialReportAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMobileAnalyticsFinancialReportAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC

- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMobileAnalyticsFullAccess

Descrizione: fornisce l'accesso completo a tutte le risorse dell'applicazione.

AmazonMobileAnalyticsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMobileAnalyticsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMobileAnalyticsNon-financialReportAccess

Descrizione: fornisce l'accesso in sola lettura ai report non finanziari per tutte le risorse dell'applicazione.

AmazonMobileAnalyticsNon-financialReportAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMobileAnalyticsNon-financialReportAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMobileAnalyticsWriteOnlyAccess

Descrizione: fornisce l'accesso in sola scrittura ai dati degli eventi put per tutte le risorse dell'applicazione. (Consigliato per l'integrazione con SDK)

AmazonMobileAnalyticsWriteOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMobileAnalyticsWriteOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMonitronFullAccess

Descrizione: Fornisce l'accesso completo per gestire Amazon Monitron

AmazonMonitronFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMonitronFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2020, 22:40 UTC
- Ora modificata: 08 giugno 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : [
          "monitron.*.amazonaws.com"
        ]
      },
      "Bool" : {
        "kms:GrantIsForAWSResource" : true
      }
    }
  },
  {
    "Sid" : "AWSSSOPermissions",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "ds:DescribeDirectories",
      "ds:DescribeTrusts"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:DescribeStream",
      "kinesis:ListStreams"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs:GetLogEvents",
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMQApiFullAccess

Descrizione: fornisce l'accesso completo ad AmazonMQ tramite la nostra API/SDK.

AmazonMQApiFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonMQApiFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 dicembre 2018, 20:31 UTC
- Ora modificata: 04 novembre 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMQApiReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad AmazonMQ tramite la nostra API/SDK.

AmazonMQApiReadOnlyAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonMQApiReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 dicembre 2018, 20:31 UTC
- Ora modificata: 18 dicembre 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMQFullAccess

Descrizione: fornisce l'accesso completo ad AmazonMQ tramite AWS Management Console

AmazonMQFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMQFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2017, 15:28 UTC
- Ora modificata: 04 novembre 2020, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMQReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad AmazonMQ tramite AWS Management Console

AmazonMQReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMQReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2017, 15:30 UTC
- Ora modificata: 28 novembre 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMQServiceRolePolicy

Descrizione: Policy Service Linked Role per AWS Amazon MQ

AmazonMQServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 4 novembre 2020, 16:07 UTC
- Ora modificata: 04 novembre 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMSKConnectReadOnlyAccess

Descrizione: Fornisci accesso in sola lettura ad Amazon MSK Connect

AmazonMSKConnectReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMSKConnectReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 settembre 2021, 10:18 UTC
- Ora modificata: 18 ottobre 2021, 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
      ]
    }
  ]
}
```

```
]
  }
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMSKFullAccess

Descrizione: Fornisci l'accesso completo ad Amazon MSK e ad altre autorizzazioni richieste per le sue dipendenze.

AmazonMSKFullAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonMSKFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 gennaio 2019, 22:07 UTC
- Ora modificata: 18 ottobre 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMSKReadOnlyAccess

Descrizione: Fornisci l'accesso in sola lettura ad Amazon MSK

AmazonMSKReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonMSKReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 gennaio 2019, 22:28 UTC
- Ora modificata: 14 gennaio 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonMWAAServiceRolePolicy

Descrizione: il ruolo collegato al servizio utilizzato da Amazon Managed Workflows per Apache Airflow.

AmazonMWAAServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 novembre 2020, 14:13 UTC
- Ora modificata: 17 novembre 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonNimbleStudio-LaunchProfileWorker

Descrizione: questa politica consente l'accesso alle risorse necessarie ai lavoratori di Nimble Studio Launch Profile. Allega questa policy alle istanze EC2 create da Nimble Studio Builder.

AmazonNimbleStudio-LaunchProfileWorker [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonNimbleStudio-LaunchProfileWorker ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 aprile 2021, 04:47 UTC
- Ora modificata: 28 aprile 2021, 04:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonNimbleStudio-StudioAdmin

Descrizione: questa politica consente l'accesso alle risorse di Amazon Nimble Studio associate all'amministratore dello studio e alle risorse di studio correlate in altri servizi. Allega questa policy al ruolo di amministratore associato al tuo studio.

AmazonNimbleStudio-StudioAdmin è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonNimbleStudio-StudioAdmin ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 aprile 2021, 04:47 UTC
- Ora modificata: 22 settembre 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonNimbleStudio-StudioUser

Descrizione: questa politica consente l'accesso alle risorse di Amazon Nimble Studio associate all'utente dello studio e alle risorse di studio correlate in altri servizi. Allega questa politica al ruolo Utente associato al tuo studio.

AmazonNimbleStudio-StudioUser è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonNimbleStudio-StudioUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 aprile 2021, 04:48 UTC
- Ora modificata: 22 settembre 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOmicsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Omics e ad altri requisiti richiesti. Servizi AWS
Questa politica consente all'utente di visualizzare e accettare gli inviti alla condivisione RAM per accedere a risorse esterne a quelle dell'utente. Account AWS

AmazonOmicsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOmicsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 24 febbraio 2023, 00:59 UTC
- Ora modificata: 24 febbraio 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"  
  }  
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOmicsReadOnlyAccess

Descrizione: Fornisci l'accesso in sola lettura ad Amazon Omics

AmazonOmicsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOmicsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2022, 04:17 UTC
- Ora modificata: 29 novembre 2022, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOneEnterpriseFullAccess

Descrizione: questa politica concede autorizzazioni amministrative che consentono l'accesso a tutte le risorse e le operazioni di Amazon One Enterprise.

AmazonOneEnterpriseFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOneEnterpriseFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2023, 04:58 UTC
- Ora modificata: 28 novembre 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOneEnterpriseInstallerAccess

Descrizione: questa politica concede autorizzazioni di lettura e scrittura limitate che consentono l'installazione e l'attivazione del dispositivo.

AmazonOneEnterpriseInstallerAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOneEnterpriseInstallerAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2023, 05:00 UTC
- Ora modificata: 28 novembre 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQRCode",
        "one:GetDeviceInstance",
        "one:GetSite",
```

```
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOneEnterpriseReadOnlyAccess

Descrizione: questa politica concede autorizzazioni di sola lettura a tutte le risorse e le operazioni di Amazon One Enterprise.

AmazonOneEnterpriseReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOneEnterpriseReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2023, 04:59 UTC
- Ora modificata: 28 novembre 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchDashboardsServiceRolePolicy

Descrizione: Fornisce l'accesso ad Amazon OpenSearch Dashboards Service per accedere ad altri AWS servizi, ad esempio per tuo CloudWatch conto

AmazonOpenSearchDashboardsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 22 dicembre 2023, 19:38 UTC
- Ora modificata: 22 dicembre 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchDirectQueryGlueCreateAccess

Descrizione: consente a OpenSearch DirectQuery Service di accedere alle API AWS Glue per creare risorse per tuo conto.

AmazonOpenSearchDirectQueryGlueCreateAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOpenSearchDirectQueryGlueCreateAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 maggio 2024, 12:24 UTC
- Ora modificata: 06 maggio 2024, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ]
    }
  ],
}
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchIngestionFullAccess

Descrizione: consente ad Amazon OpenSearch Ingestion di accedere ad altri AWS servizi per tuo conto.

AmazonOpenSearchIngestionFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOpenSearchIngestionFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 aprile 2023, 18:11 UTC
- Ora modificata: 26 aprile 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchIngestionReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon OpenSearch Ingestion Service

AmazonOpenSearchIngestionReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOpenSearchIngestionReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 aprile 2023, 18:09 UTC
- Ora modificata: 26 aprile 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchIngestionServiceRolePolicy

Descrizione: consente ad Amazon OpenSearch Ingestion Service di accedere ad altri AWS servizi per tuo conto.

AmazonOpenSearchIngestionServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 novembre 2022, 16:49 UTC
- Ora modificata: 18 novembre 2022, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchServerlessServiceRolePolicy

Descrizione: consenti ad Amazon OpenSearch Serverless di accedere ad altri AWS servizi come le CloudWatch API per tuo conto.

AmazonOpenSearchServerlessServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 novembre 2022, 19:50 UTC
- Ora modificata: 24 novembre 2022, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchServiceCognitoAccess

Descrizione: fornisce l'accesso al servizio di configurazione Amazon Cognito.

AmazonOpenSearchServiceCognitoAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOpenSearchServiceCognitoAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 settembre 2021, 06:31 UTC
- Ora modificata: 20 dicembre 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchServiceFullAccess

Descrizione: fornisce l'accesso completo al servizio di configurazione OpenSearch di Amazon Service.

AmazonOpenSearchServiceFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOpenSearchServiceFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 08 settembre 2021, 05:33 UTC
- Ora modificata: 08 settembre 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchServiceReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio di configurazione di Amazon OpenSearch Service.

AmazonOpenSearchServiceReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonOpenSearchServiceReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 08 settembre 2021, 05:38 UTC
- Ora modificata: 08 settembre 2021, 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonOpenSearchServiceRolePolicy

Descrizione: consenti ad Amazon OpenSearch Service di accedere ad altri AWS servizi come le API di rete EC2 per tuo conto.

AmazonOpenSearchServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 agosto 2021, 09:27 UTC
- Ora modificata: 23 ottobre 2023, 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonPersonalizeFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Personalize tramite l'SDK AWS Management Console and. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3, CloudWatch).

AmazonPersonalizeFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonPersonalizeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 4 dicembre 2018, 22:24 UTC
- Ora modificata: 30 maggio 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"  
  }  
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonPollyFullAccess

Descrizione: garantisce l'accesso completo al servizio e alle risorse Amazon Polly.

AmazonPollyFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonPollyFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 18:59 UTC
- Ora modificata: 30 novembre 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonPollyReadOnlyAccess

Descrizione: concede l'accesso in sola lettura alle risorse di Amazon Polly.

AmazonPollyReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonPollyReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 18:59 UTC
- Ora modificata: 17 luglio 2018, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonPrometheusConsoleFullAccess

Descrizione: concede l'accesso completo alle risorse AWS gestite di Prometheus nella console AWS

AmazonPrometheusConsoleFullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonPrometheusConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 18:11 UTC
- Ora modificata: 24 ottobre 2022, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonPrometheusFullAccess

Descrizione: Garantisce l'accesso completo alle risorse AWS gestite di Prometheus

AmazonPrometheusFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonPrometheusFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 18:10 UTC
- Ora modificata: 26 novembre 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonPrometheusQueryAccess

Descrizione: concede l'accesso per eseguire query sulle risorse gestite di AWS Prometheus

AmazonPrometheusQueryAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonPrometheusQueryAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 dicembre 2020, 01:02 UTC
- Ora modificata: 19 dicembre 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonPrometheusRemoteWriteAccess

Descrizione: concede l'accesso in sola scrittura alle aree di lavoro AWS gestite di Prometheus

AmazonPrometheusRemoteWriteAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonPrometheusRemoteWriteAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 dicembre 2020, 01:04 UTC
- Ora modificata: 19 dicembre 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Action" : [
      "aps:RemoteWrite"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonPrometheusScrapperServiceRolePolicy

Descrizione: Fornisce l'accesso alle AWS risorse gestite o utilizzate da Amazon Managed Service per Prometheus Collector

AmazonPrometheusScrapperServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 novembre 2023, 14:19 UTC
- Ora modificata: 26 aprile 2024, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScrapperServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "Null" : {
        "aws:RequestTag/AMPAgentlessScraper" : "false"
      }
    }
  },
  {
    "Sid" : "ENIUpdating",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AMPAgentlessScraper" : "false"
      }
    }
  },
  {
    "Sid" : "EKSAccess",
    "Effect" : "Allow",
    "Action" : "eks:DescribeCluster",
    "Resource" : "arn:aws:eks:*:*:cluster/*"
  },
  {
    "Sid" : "DeleteEKSAccessEntry",
    "Effect" : "Allow",
    "Action" : "eks:DeleteAccessEntry",
    "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
}

```

```
    },
    "ArnLike" : {
      "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
    }
  },
  {
    "Sid" : "APSWriting",
    "Effect" : "Allow",
    "Action" : "aps:RemoteWrite",
    "Resource" : "arn:aws:aps:*:*:workspace/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonQFullAccess

Descrizione: Fornisce accesso completo per abilitare le interazioni con Amazon Q

AmazonQFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonQFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2023, 16:00 UTC

- Ora modificata: 29 aprile 2024, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonQLDBConsoleFullAccess

Descrizione: fornisce l'accesso completo ad Amazon QLDB tramite AWS Management Console.

AmazonQLDBConsoleFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonQLDBConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 settembre 2019, 18:24 UTC
- Ora modificata: 04 novembre 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonQLDBFullAccess

Descrizione: fornisce l'accesso completo ad Amazon QLDB tramite l'API del servizio.

AmazonQLDBFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonQLDBFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 settembre 2019, 18:23 UTC

- Ora modificata: 04 novembre 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonQLDBReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon QLDB.

AmazonQLDBReadOnly è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonQLDBReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 settembre 2019, 18:19 UTC
- Ora modificata: 02 luglio 2021, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSBetaServiceRolePolicy

Descrizione: consente ad Amazon RDS di gestire AWS le risorse per tuo conto.

AmazonRDSBetaServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 2 maggio 2018, 19:41 UTC
- Ora modificata: 14 dicembre 2022, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSCustomInstanceProfileRolePolicy

Descrizione: consente ad Amazon RDS Custom di eseguire varie azioni di automazione e attività di gestione del database tramite un profilo di istanza EC2.

AmazonRDSCustomInstanceProfileRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRDSCustomInstanceProfileRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 febbraio 2024, 17:42 UTC
- Ora modificata: 27 febbraio 2024, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSCustomPreviewServiceRolePolicy

Descrizione: politica del ruolo del servizio Amazon RDS Custom Preview

AmazonRDSCustomPreviewServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 8 ottobre 2021, 21:44 UTC
- Ora modificata: 20 settembre 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSCustomServiceRolePolicy

Descrizione: consente ad Amazon RDS Custom di gestire AWS le risorse per tuo conto.

AmazonRDSCustomServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 8 ottobre 2021, 21:39 UTC

- Ora modificata: 19 aprile 2024, 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
```



```

        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "ecc2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "ecc1scoping",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AllocateAddress"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringLike" : {

```

```

        "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
        ]
    },
    {
        "Sid" : "ecc1scoping2",
        "Effect" : "Allow",
        "Action" : [
            "ec2:AssociateAddress",
            "ec2:DisassociateAddress",
            "ec2:ReleaseAddress"
        ],
        "Resource" : [
            "*"
        ],
        "Condition" : {
            "StringLike" : {
                "aws:ResourceTag/AWSRDSCustom" : [
                    "custom-oracle",
                    "custom-sqlserver",
                    "custom-oracle-rac"
                ]
            }
        }
    },
    {
        "Sid" : "ecc1scoping3",
        "Effect" : "Allow",
        "Action" : [
            "ec2:AssignPrivateIpAddresses"
        ],
        "Resource" : "arn:aws:ec2:*:*:network-interface/*",
        "Condition" : {
            "StringLike" : {
                "aws:ResourceTag/AWSRDSCustom" : [
                    "custom-oracle-rac"
                ]
            }
        }
    }
},

```

```

{
  "Sid" : "eccRunInstances1",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
    "arn:aws:ec2:*:*:placement-group/*"
  ]
},
{
  "Sid" : "eccRunInstances3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {

```

```

        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle-rac",
                "custom-oracle"
            ]
        }
    },
    {
        "Sid" : "eccModifyInstanceAttribute1",
        "Effect" : "Allow",
        "Action" : [
            "ec2:ModifyInstanceAttribute"
        ],
        "Resource" : [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Condition" : {
            "StringEquals" : {
                "aws:ResourceTag/AWSRDSCustom" : [
                    "custom-sqlserver"
                ],
                "ec2:Attribute" : "InstanceType"
            }
        }
    },
    {
        "Sid" : "RequireImdsV2",
        "Effect" : "Deny",
        "Action" : "ec2:RunInstances",
        "Resource" : "arn:aws:ec2:*:*:instance/*",
        "Condition" : {
            "StringNotEquals" : {
                "ec2:MetadataHttpTokens" : "required"
            },
            "StringLike" : {
                "aws:RequestTag/AWSRDSCustom" : [
                    "custom-oracle-rac"
                ]
            }
        }
    },
    {
        "Sid" : "eccRunInstances3keyPair1",

```

```

    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances",
        "ec2>DeleteKeyPair"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
    ],
    "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*",
        "arn:aws:iam:*:*:role/service-role/AWSRDSCustom*"
    ],

```

```
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    },
  },
  {
    "Sid" : "cloudtrail1",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:GetTrailStatus"
    ],
    "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
  },
  {
    "Sid" : "cw1",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:EnableAlarmActions",
      "cloudwatch:DeleteAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "cw2",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:TagResource"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
```

```

        "custom-sqlserver",
        "custom-oracle-rac"
    ]
}
},
{
    "Sid" : "cw3",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
},
{
    "Sid" : "ssm1",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws:ssm:*:*:document/*"
},
{
    "Sid" : "ssm2",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "ssm3",
    "Effect" : "Allow",
    "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
    ],
    "Resource" : "*"
}

```

```
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm>DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
        "custom-sqlserver",
        "custom-oracle-rac"
    ]
}
},
{
    "Sid" : "eb2",
    "Effect" : "Allow",
    "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "eb3",
    "Effect" : "Allow",
    "Action" : [
        "events:PutRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
        "StringLike" : {
            "events:ManagedBy" : [
                "custom.rds.amazonaws.com"
            ]
        }
    }
},
```

```

{
  "Sid" : "eb4",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:EnableRule",
    "events>DeleteRule",
    "events:RemoveTargets",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "events:ManagedBy" : [
        "custom.rds.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "eb5",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
},
{
  "Sid" : "secretmanager1",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:TagResource",
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
  "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" : "*"
    }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSDDataFullAccess

Descrizione: consente l'accesso completo all'utilizzo delle API dei dati RDS, delle API dell'archivio segreto per le credenziali del database RDS e delle API di gestione delle query della console DB per eseguire istruzioni SQL sui cluster Aurora Serverless in Account AWS

AmazonRDSDDataFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRDSDDataFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2018, 21:29 UTC
- Ora modificata: 20 novembre 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSDirectoryServiceAccess

Descrizione: consente a RDS di accedere a Directory Service Managed AD per conto del cliente per le istanze DB di SQL Server aggiunte al dominio.

AmazonRDSDirectoryServiceAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRDSDirectoryServiceAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 febbraio 2016, 02:02 UTC
- Ora modificata: 15 maggio 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSEnhancedMonitoringRole

Descrizione: fornisce l'accesso a Cloudwatch for RDS Enhanced Monitoring

AmazonRDSEnhancedMonitoringRole è [una policy gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonRDSEnhancedMonitoringRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 novembre 2015, 19:58 UTC
- Ora modificata: 11 novembre 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSFullAccess

Descrizione: fornisce l'accesso completo ad Amazon RDS tramite AWS Management Console

AmazonRDSFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRDSFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 17 agosto 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSPerformanceInsightsFullAccess

Descrizione: Fornisce l'accesso completo a RDS Performance Insights tramite AWS Management Console

AmazonRDSPerformanceInsightsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRDSPerformanceInsightsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 agosto 2023, 23:41 UTC
- Ora modificata: 23 ottobre 2023, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSPerformanceInsightsReadOnly

Descrizione: policy di sola lettura per RDS Performance Insights

AmazonRDSPerformanceInsightsReadOnly è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonRDSPerformanceInsightsReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 5 aprile 2022, 00:02 UTC
- Ora modificata: 23 ottobre 2023, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSPreviewServiceRolePolicy

Descrizione: Politica sul ruolo del servizio Amazon RDS Preview

AmazonRDSPreviewServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 31 maggio 2018, 18:02 UTC
- Ora modificata: 04 ottobre 2023, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon RDS tramite AWS Management Console

AmazonRDSReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRDSReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 14 aprile 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRDSServiceRolePolicy

Descrizione: consente ad Amazon RDS di gestire AWS le risorse per tuo conto.

AmazonRDSServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 8 gennaio 2018, 18:17 UTC
- Ora modificata: 19 gennaio 2024, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```


Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftAllCommandsFullAccess

Descrizione: questa policy include le autorizzazioni per eseguire comandi SQL per copiare, caricare, scaricare, interrogare e analizzare i dati su Amazon Redshift. La policy concede inoltre le autorizzazioni per eseguire istruzioni selezionate per servizi correlati, come Amazon S3, Amazon logs, CloudWatch SageMaker Amazon o Glue. AWS

AmazonRedshiftAllCommandsFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftAllCommandsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 04 novembre 2021, 00:48 UTC
- Ora modificata: 25 novembre 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftDataFullAccess

Descrizione: questa policy fornisce l'accesso completo alle API dei dati di Amazon Redshift. Questa policy garantisce anche l'accesso mirato ad altri servizi richiesti.

AmazonRedshiftDataFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftDataFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 settembre 2020, 19:23 UTC
- Ora modificata: 07 aprile 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Redshift tramite. AWS Management Console

AmazonRedshiftFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 07 luglio 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftQueryEditor

Descrizione: fornisce l'accesso completo ad Amazon Redshift Query Editor e alle query salvate tramite AWS Management Console

AmazonRedshiftQueryEditor è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftQueryEditor ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 ottobre 2018, 22:50 UTC
- Ora modificata: 16 febbraio 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftQueryEditorV2FullAccess

Descrizione: concede l'accesso completo alle operazioni e alle risorse di Amazon Redshift Query Editor V2. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Ciò include le autorizzazioni per elencare i cluster Amazon Redshift, leggere chiavi e alias AWS in KMS e gestire i segreti di Query Editor V2 in Secrets Manager. AWS

AmazonRedshiftQueryEditorV2FullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftQueryEditorV2FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 settembre 2021, 14:06 UTC
- Ora modificata: 21 febbraio 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftQueryEditorV2NoSharing

Descrizione: consente di lavorare con Amazon Redshift Query Editor V2 senza condividere risorse. Il titolare autorizzato può solo leggere, aggiornare ed eliminare le proprie risorse, ma non può condividerle. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Ciò include le autorizzazioni per elencare i cluster Amazon Redshift e gestire i segreti di Query Editor V2 del principale in Secrets Manager. AWS

AmazonRedshiftQueryEditorV2NoSharing è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftQueryEditorV2NoSharing ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 settembre 2021, 14:18 UTC
- Ora modificata: 21 febbraio 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftQueryEditorV2ReadSharing

Descrizione: consente di lavorare con Amazon Redshift Query Editor V2 con una condivisione limitata delle risorse. Il titolare autorizzato può leggere, scrivere e condividere le proprie risorse. Il responsabile autorizzato può leggere le risorse condivise con il suo team ma non può aggiornarle. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Ciò include le autorizzazioni per elencare i cluster Amazon Redshift e gestire i segreti di Query Editor V2 del principale in Secrets Manager. AWS

AmazonRedshiftQueryEditorV2ReadSharing [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftQueryEditorV2ReadSharing ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 24 settembre 2021, 14:22 UTC
- Ora modificata: 21 febbraio 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "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}"
        }
    }
}

```

```
}  
  }  
    }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

Descrizione: consente di utilizzare Amazon Redshift Query Editor V2 con condivisione di risorse. Il titolare autorizzato può leggere, scrivere e condividere le proprie risorse. Il principale concesso può leggere e aggiornare le risorse condivise con il suo team. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Ciò include le autorizzazioni per elencare i cluster Amazon Redshift e gestire i segreti di Query Editor V2 del principale in Secrets Manager. AWS

AmazonRedshiftQueryEditorV2ReadWriteSharing è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftQueryEditorV2ReadWriteSharing ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 settembre 2021, 14:25 UTC
- Ora modificata: 21 febbraio 2024, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
```

```

    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateFolder",
      "sqlworkbench:PutTab",
      "sqlworkbench:BatchDeleteFolder",
      "sqlworkbench>DeleteTab",
      "sqlworkbench:GenerateSession",
      "sqlworkbench:GetAccountInfo",
      "sqlworkbench:GetAccountSettings",
      "sqlworkbench:GetUserInfo",
      "sqlworkbench:GetUserWorkspaceSettings",
      "sqlworkbench:PutUserWorkspaceSettings",
      "sqlworkbench>ListConnections",
      "sqlworkbench>ListFiles",
      "sqlworkbench>ListTabs",
      "sqlworkbench:UpdateFolder",
      "sqlworkbench>ListRedshiftClusters",
      "sqlworkbench:DriverExecute",
      "sqlworkbench>ListTaggedResources",
      "sqlworkbench>ListQueryExecutionHistory",
      "sqlworkbench:GetQueryExecutionHistory",
      "sqlworkbench>ListNotebooks",
      "sqlworkbench:GetSchemaInference",
      "sqlworkbench:GetAutocompletionMetadata",
      "sqlworkbench:GetAutocompletionResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateConnection",
      "sqlworkbench:CreateSavedQuery",
      "sqlworkbench:CreateChart",
      "sqlworkbench:CreateNotebook",
      "sqlworkbench:DuplicateNotebook",

```

```

        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
    }
},
{
    "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
    "Effect" : "Allow",
    "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
    ]
}

```

```

        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
    }
},
{
    "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
    "Effect" : "Allow",
    "Action" : "sqlworkbench:TagResource",
    "Resource" : "*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
            "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
            "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
    }
},
{
    "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
    "Effect" : "Allow",
    "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
    ]
}

```



```

        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
    }
},
{
    "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
    "Effect" : "Allow",
    "Action" : "sqlworkbench:TagResource",
    "Resource" : "*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
            "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
            "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
    }
},
{
    "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
    "Effect" : "Allow",
    "Action" : "sqlworkbench:UntagResource",
    "Resource" : "*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
            "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
    }
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Redshift tramite AWS Management Console

AmazonRedshiftReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRedshiftReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 08 febbraio 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRedshiftServiceLinkedRolePolicy

Descrizione: consente ad Amazon Redshift di chiamare i AWS servizi per tuo conto

AmazonRedshiftServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 settembre 2017, 19:19 UTC
- Ora modificata: 15 marzo 2024, 20:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRekognitionCustomLabelsFullAccess

Descrizione: questa politica specifica le autorizzazioni Rekognition e s3 richieste dalla funzionalità Amazon Rekognition Custom Labels.

AmazonRekognitionCustomLabelsFullAccess [AWS è una politica](#) gestita.

Utilizzo di questa politica

Puoi collegarti AmazonRekognitionCustomLabelsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 gennaio 2020, 19:18 UTC
- Ora modificata: 16 agosto 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRekognitionFullAccess

Descrizione: Accesso a tutte le API di Amazon Rekognition

AmazonRekognitionFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRekognitionFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 14:40 UTC
- Ora modificata: 30 novembre 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRekognitionReadOnlyAccess

Descrizione: accesso a tutte le API di riconoscimento di Read

AmazonRekognitionReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRekognitionReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 14:58 UTC
- Ora modificata: 08 novembre 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRekognitionServiceRole

Descrizione: consente a Rekognition di chiamare i servizi per AWS tuo conto.

AmazonRekognitionServiceRole è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonRekognitionServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 novembre 2017, 16:52 UTC
- Ora modificata: 29 novembre 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53AutoNamingFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni di denominazione automatica della Route 53.

AmazonRoute53AutoNamingFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53AutoNamingFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2018, 18:40 UTC
- Ora modificata: 18 gennaio 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53AutoNamingReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutte le azioni di denominazione automatica della Route 53.

AmazonRoute53AutoNamingReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53AutoNamingReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2018, 03:02 UTC
- Ora modificata: 18 gennaio 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53AutoNamingRegistrantAccess

Descrizione: fornisce l'accesso a livello di registrante alle azioni di denominazione automatica della Route 53.

AmazonRoute53AutoNamingRegistrantAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53AutoNamingRegistrantAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 marzo 2018, 22:33 UTC
- Ora modificata: 12 marzo 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53DomainsFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni di Route53 Domains e Create Hosted Zone per consentire la creazione di Hosted Zone come parte delle registrazioni di domini.

AmazonRoute53DomainsFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonRoute53DomainsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53DomainsReadOnlyAccess

Descrizione: fornisce l'accesso all'elenco e alle azioni dei domini Route53.

AmazonRoute53DomainsReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53DomainsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53FullAccess

Descrizione: fornisce l'accesso completo a tutte le Amazon Route 53 tramite AWS Management Console.

AmazonRoute53FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 20 dicembre 2018, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53ProfilesFullAccess

Descrizione: questa politica garantisce l'accesso completo alle risorse del profilo Amazon Route 53.

AmazonRoute53ProfilesFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53ProfilesFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 30 aprile 2024, 18:30 UTC
- Ora modificata: 30 aprile 2024, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles>DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
```

```
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53ProfilesReadOnlyAccess

Descrizione: questa policy garantisce l'accesso in sola lettura alle risorse del profilo Amazon Route 53.

AmazonRoute53ProfilesReadOnlyAccess [è una policy gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53ProfilesReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 aprile 2024, 18:29 UTC
- Ora modificata: 30 aprile 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53ReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutte le Amazon Route 53 tramite AWS Management Console.

AmazonRoute53ReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 15 novembre 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
```

```
    "route53:List*",
    "route53:TestDNSAnswer"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53RecoveryClusterFullAccess

Descrizione: Fornisce accesso completo ad Amazon Route 53 Recovery Cluster

AmazonRoute53RecoveryClusterFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53RecoveryClusterFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 18:37 UTC
- Ora modificata: 18 agosto 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon Route 53 Recovery Cluster

AmazonRoute53RecoveryClusterReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53RecoveryClusterReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 18 agosto 2021, 17:36 UTC
- Ora modificata: 01 aprile 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53RecoveryControlConfigFullAccess

Descrizione: Fornisce accesso completo ad Amazon Route 53 Recovery Control Config

AmazonRoute53RecoveryControlConfigFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53RecoveryControlConfigFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 17:48 UTC
- Ora modificata: 18 agosto 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon Route 53 Recovery Control Config

AmazonRoute53RecoveryControlConfigReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53RecoveryControlConfigReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 18:01 UTC
- Ora modificata: 18 ottobre 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53RecoveryReadinessFullAccess

Descrizione: Fornisce accesso completo ad Amazon Route 53 Recovery Readiness

AmazonRoute53RecoveryReadinessFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53RecoveryReadinessFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 16:45 UTC
- Ora modificata: 18 agosto 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon Route 53 Recovery Readiness

AmazonRoute53RecoveryReadinessReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53RecoveryReadinessReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 18:11 UTC
- Ora modificata: 09 novembre 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53ResolverFullAccess

Descrizione: Politica di accesso completo per Route 53 Resolver

AmazonRoute53ResolverFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53ResolverFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2019, 18:10 UTC
- Ora modificata: 17 luglio 2020, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonRoute53ResolverReadOnlyAccess

Descrizione: Politica di sola lettura per Route 53 Resolver

AmazonRoute53ResolverReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonRoute53ResolverReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2019, 18:11 UTC
- Ora modificata: 27 settembre 2019, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "route53resolver:Get*",
      "route53resolver:List*",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonS3FullAccess

Descrizione: fornisce l'accesso completo a tutti i bucket tramite AWS Management Console

AmazonS3FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonS3FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC

- Ora modificata: 27 settembre 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonS3ObjectLambdaExecutionRolePolicy

Descrizione: fornisce le autorizzazioni per le funzioni AWS Lambda per interagire con Amazon S3 Object Lambda. Concede inoltre le autorizzazioni Lambda per la scrittura nei registri. CloudWatch

AmazonS3ObjectLambdaExecutionRolePolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonS3ObjectLambdaExecutionRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 agosto 2021, 10:07 UTC
- Ora modificata: 18 agosto 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonS3OutpostsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon S3 on Outposts tramite AWS Management Console

AmazonS3OutpostsFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonS3OutpostsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 ottobre 2020, 17:26 UTC
- Ora modificata: 2 ottobre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonS3OutpostsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon S3 on Outposts tramite. AWS Management Console

AmazonS3OutpostsReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonS3OutpostsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 ottobre 2020, 18:55 UTC
- Ora modificata: 2 ottobre 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonS3ReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutti i bucket tramite AWS Management Console

AmazonS3ReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonS3ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 10 agosto 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ]
    }
  ]
}
```



```
    ],  
    "Resource" : "*"br/>  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata dal servizio Servizio AWS Catalog per fornire prodotti del SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a una serie di servizi correlati tra cui CodePipeline, CodeBuild,, CodeCommit Glue CloudFormation, ecc.

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2020, 18:48 UTC
- Ora modificata: 12 giugno 2024, 18:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "codecommit:ListRepositories"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
    ],
    "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
    ]
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringLike" : {
            "aws:TagKeys" : [
                "sagemaker:launch-source"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp>DeleteGroup",
        "cognito-idp>DeleteUserPool",
        "cognito-idp>DeleteUserPoolClient",
        "cognito-idp>DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ecr:CreateRepository",
        "ecr>DeleteRepository",
        "ecr:TagResource"
    ],
    "Resource" : [

```

```

        "arn:aws:ecr:*:*:repository/sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "events:DescribeRule",
        "events>DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "firehose>CreateDeliveryStream",
        "firehose>DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
    ],
    "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue>CreateDatabase",
        "glue>DeleteDatabase"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
    ]
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
        "glue:CreateClassifier",
        "glue>DeleteClassifier",
        "glue>DeleteCrawler",
        "glue>DeleteJob",
        "glue>DeleteTrigger",
        "glue>DeleteWorkflow",
        "glue:StopCrawler"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateWorkflow"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateJob"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
    ]
},
{
    "Effect" : "Allow",

```

```

    "Action" : [
      "glue:CreateTrigger",
      "glue:GetTrigger"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:trigger/sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonSageMakerServiceCatalog*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:AddPermission",
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:GetFunction",
      "lambda:GetFunctionConfiguration",
      "lambda:InvokeFunction",
      "lambda:RemovePermission"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "lambda:TagResource",
    "Resource" : [
      "arn:aws:lambda:*:*:function:sagemaker-*"
    ],
    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : [
          "sagemaker:*"
        ]
      }
    }
  }
}

```



```

    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs>DeleteLogGroup",
      "logs>DeleteLogStream",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs:PutRetentionPolicy"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
      "arn:aws:logs:*:*:log-group::log-stream:*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : [
      "arn:aws:s3:::sagemaker-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3>DeleteBucket",
      "s3>DeleteBucketPolicy",
      "s3:GetBucketPolicy",
      "s3:PutBucketAcl",
      "s3:PutBucketNotification",

```

```

        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
    ],
    "Resource" : "arn:aws:s3::sagemaker-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker>DeleteEndpoint",
        "sagemaker>DeleteEndpointConfig",
        "sagemaker>DeleteModel",
        "sagemaker>DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker>DeleteCodeRepository"
    ],
    "Resource" : [
        "arn:aws:sagemaker:*:*:*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:AddTags"
    ],
    "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",

```

```

        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
    ],
    "Condition" : {
        "ForAllValues:StringLike" : {
            "aws:TagKeys" : [
                "sagemaker:*"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreateImage",
        "sagemaker>DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
    ],
    "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "states:CreateStateMachine",
        "states>DeleteStateMachine",
        "states:UpdateStateMachine"
    ],
    "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : "codestar-connections:PassConnection",
    "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
    "Condition" : {
        "StringEquals" : {
            "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
    }
}

```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerCanvasAIServiceAccess

Descrizione: fornisce le autorizzazioni ad Amazon SageMaker Canvas per utilizzare i servizi di intelligenza artificiale per supportare soluzioni AI pronte all'uso. Questa politica aggiungerà ulteriori autorizzazioni mutanti per i servizi man mano che Amazon SageMaker Canvas aggiungerà il supporto.

AmazonSageMakerCanvasAIServiceAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerCanvasAIServiceAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2023, 22:36 UTC
- Ora modificata: 29 novembre 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServiceAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
}

```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerCanvasBedrockAccess

Descrizione: questa politica concede le autorizzazioni per utilizzare Amazon Bedrock in SageMaker Canvas fornendo l'accesso a servizi downstream come S3.

AmazonSageMakerCanvasBedrockAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerCanvasBedrockAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 febbraio 2024, 18:37 UTC
- Ora modificata: 02 febbraio 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerCanvasDataPrepFullAccess

Descrizione: fornisce l'accesso completo alle SageMaker risorse e alle operazioni di Amazon per la preparazione dei dati in Canvas. La policy fornisce anche un accesso selezionato ai servizi correlati (ad esempio, S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue, Secrets Manager). EventBridge Questa policy deve essere allegata al ruolo di esecuzione Amazon SageMaker Domain/ User Profile.

AmazonSageMakerCanvasDataPrepFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerCanvasDataPrepFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 ottobre 2023, 22:56 UTC
- Ora modificata: 08 dicembre 2023, 02:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerCanvasDirectDeployAccess

Descrizione: consente ad Amazon SageMaker Canvas di creare, gestire e visualizzare i dettagli degli endpoint per gli endpoint creati tramite Canvas. Consente ad Amazon SageMaker Canvas di recuperare i parametri di chiamata degli endpoint da CloudWatch

AmazonSageMakerCanvasDirectDeployAccess [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerCanvasDirectDeployAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 ottobre 2023, 18:11 UTC
- Ora modificata: 6 ottobre 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerCanvasForecastAccess

Descrizione: questa politica concede le autorizzazioni comunemente necessarie per utilizzare SageMaker Canvas con Amazon Forecast.

AmazonSageMakerCanvasForecastAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerCanvasForecastAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 agosto 2022, 20:04 UTC
- Ora modificata: 24 agosto 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
      ]
    }
  ]
}
```

```
]
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerCanvasFullAccess

Descrizione: fornisce l'accesso completo alle risorse e alle operazioni di Amazon SageMaker Canvas. La policy fornisce anche un accesso selezionato ai servizi correlati (ad esempio, S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager e Forecast). Questa policy deve essere allegata al ruolo di esecuzione Amazon SageMaker Domain/User Profile.

AmazonSageMakerCanvasFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerCanvasFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 09 settembre 2022, 00:44 UTC
- Ora modificata: 24 gennaio 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerClusterInstanceRolePolicy

Descrizione: questa politica concede le autorizzazioni comunemente necessarie per utilizzare Amazon SageMaker Cluster.

AmazonSageMakerClusterInstanceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerClusterInstanceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2023, 15:11 UTC
- Ora modificata: 29 novembre 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerCoreServiceRolePolicy

Descrizione: policy gestita per Service Linked Role for Amazon SageMaker Core Services

AmazonSageMakerCoreServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 dicembre 2020, 21:40 UTC
- Ora modificata: 21 dicembre 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  },
  "Action" : [
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerEdgeDeviceFleetPolicy

Descrizione: fornisce le autorizzazioni necessarie a SageMaker Edge per creare e gestire una flotta di dispositivi per il cliente utilizzando la connessione cloud predefinita.

AmazonSageMakerEdgeDeviceFleetPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerEdgeDeviceFleetPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 08 dicembre 2020, 16:17 UTC

- Ora modificata: 08 dicembre 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
}

```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerFeatureStoreAccess

Descrizione: fornisce le autorizzazioni necessarie per abilitare lo store offline per un gruppo di SageMaker FeatureStore funzionalità Amazon.

AmazonSageMakerFeatureStoreAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerFeatureStoreAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 16:24 UTC
- Ora modificata: 05 dicembre 2022, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SageMaker tramite l'SDK AWS Management Console and. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3, ECR, CloudWatch Logs).

AmazonSageMakerFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 13:07 UTC
- Ora modificata: 29 marzo 2024, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Versione della politica

Versione della politica: v26 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "AllowAddTagsForSpace",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:AddTags"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:space/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "sagemaker:TaggingAction" : "CreateSpace"
      }
    }
  },
  {
    "Sid" : "AllowAddTagsForApp",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:AddTags"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:app/*"
    ]
  },
  {
    "Sid" : "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:UserName}"
      },
      "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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerGeospatialExecutionRole

Descrizione: questa politica fornisce l'accesso ai servizi che sono comunemente necessari per l'uso della tecnologia SageMaker geospaziale.

AmazonSageMakerGeospatialExecutionRole [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerGeospatialExecutionRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 30 novembre 2022, 10:08 UTC
- Ora modificata: 10 maggio 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerGeospatialFullAccess

Descrizione: questa policy concede autorizzazioni che consentono l'accesso completo ad Amazon SageMaker Geospatial tramite l'SDK and. AWS Management Console

AmazonSageMakerGeospatialFullAccess [AWS è una politica](#) gestita.

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerGeospatialFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 30 novembre 2022, 10:06 UTC
- Ora modificata: 30 novembre 2022, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
          ]
        }
      }
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerGroundTruthExecution

Descrizione: fornisce l'accesso ai AWS servizi necessari per eseguire il processo di SageMaker GroundTruth etichettatura

AmazonSageMakerGroundTruthExecution è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerGroundTruthExecution ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 luglio 2020, 19:30 UTC
- Ora modificata: 29 aprile 2022, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    ]
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerMechanicalTurkAccess

Descrizione: fornisce l'accesso per creare risorse Amazon Augmented FlowDefinition AI per qualsiasi team di lavoro.

AmazonSageMakerMechanicalTurkAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerMechanicalTurkAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 03 dicembre 2019, 16:19 UTC
- Ora modificata: 03 dicembre 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerModelGovernanceUseAccess

Descrizione: questa politica AWS gestita concede le autorizzazioni necessarie per utilizzare tutte le funzionalità di Amazon SageMaker Governance. La policy fornisce anche un accesso selezionato ai servizi correlati (ad esempio, S3, KMS).

AmazonSageMakerModelGovernanceUseAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerModelGovernanceUseAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2022, 08:58 UTC
- Ora modificata: 04 giugno 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSMMonitoringModelCards",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
```

```

        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:ListModelCardExportJobs"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowSMTrainingModelsSearchTags",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
        "sagemaker:Search",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowKMSActions",
    "Effect" : "Allow",
    "Action" : [
        "kms:ListAliases"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowS3Actions",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject",

```

```
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
    ],
    "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
    ]
},
{
    "Sid" : "AllowS3ListActions",
    "Effect" : "Allow",
    "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerModelRegistryFullAccess

Descrizione: Questa è una nuova politica gestita per Model Registry in Sagemaker. Questa politica è una politica autonoma che può essere associata al ruolo utente per accedere alle funzionalità relative al Model Registry in Sagemaker.

AmazonSageMakerModelRegistryFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerModelRegistryFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 aprile 2023, 05:20 UTC
- Ora modificata: 6 giugno 2024, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
  ],
}
```

```

    "Sid" : "AmazonSageMakerModelRegistrySageMakerWritePermission",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker>DeleteModelPackage",
        "sagemaker>DeleteModelPackageGroup",
        "sagemaker>DeleteTags",
        "sagemaker:UpdateModelPackage"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AmazonSageMakerModelRegistryS3GetPermission",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
    ]
},
{
    "Sid" : "AmazonSageMakerModelRegistryS3ListPermission",
    "Effect" : "Allow",
    "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AmazonSageMakerModelRegistryECRReadPermission",
    "Effect" : "Allow",
    "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
    ]
}

```

```

    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryIAMPassRolePermission",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "sagemaker.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryTagReadPermission",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:GetGroupQuery"
    ],
    "Resource" : "arn:aws:resource-groups::*:group/*"
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:ListGroupResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
    "Effect" : "Allow",
    "Action" : [

```

```

        "resource-groups:CreateGroup",
        "resource-groups:Tag"
    ],
    "Resource" : "arn:aws:resource-groups:*:*:group/*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:TagKeys" : "sagemaker:collection"
        }
    }
},
{
    "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
    "Effect" : "Allow",
    "Action" : "resource-groups:DeleteGroup",
    "Resource" : "arn:aws:resource-groups:*:*:group/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/sagemaker:collection" : "true"
        }
    }
},
{
    "Sid" : "AmazonSageMakerModelRegistryResourceKMSPermission",
    "Effect" : "Allow",
    "Action" : [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/sagemaker" : "true"
        },
        "StringLike" : {
            "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerNotebooksServiceRolePolicy

Descrizione: policy gestita per Service Linked Role per Amazon SageMaker Notebooks

AmazonSageMakerNotebooksServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 ottobre 2019, 20:27 UTC
- Ora modificata: 22 maggio 2024, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AllowEFSAccessPointCreation",
    "Effect" : "Allow",
    "Action" : "elasticfilesystem:CreateAccessPoint",
    "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
        "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
      }
    }
  },
  {
    "Sid" : "AllowEFSAccessPointDeletion",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:DeleteAccessPoint"
    ],
    "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
      }
    }
  },
  {
    "Sid" : "AllowEFSCreation",
    "Effect" : "Allow",
    "Action" : "elasticfilesystem:CreateFileSystem",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
      }
    }
  },
  {
    "Sid" : "AllowEFSMountWithDeletion",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:CreateMountTarget",
      "elasticfilesystem:DeleteFileSystem",

```

```

        "elasticfilesystem:DeleteMountTarget"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
    }
},
{
    "Sid" : "AllowEFSDescribe",
    "Effect" : "Allow",
    "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowEFSTagging",
    "Effect" : "Allow",
    "Action" : "elasticfilesystem:TagResource",
    "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
    }
},
{
    "Sid" : "AllowEC2Tagging",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
    ]
},
{
    "Sid" : "AllowEC2Operations",

```

```

    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowEC2AuthZ",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2>DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
    }
},
{
    "Sid" : "AllowIdcOperations",
    "Effect" : "Allow",
    "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso>DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
    ],
    "Resource" : "*"
},
{

```

```

    "Sid" : "AllowSagemakerProfileCreation",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowSagemakerSpaceOperationsForCanvasManagedSpaces",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DescribeSpace",
        "sagemaker>DeleteSpace",
        "sagemaker:ListTags"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
  },
  {
    "Sid" : "AllowSagemakerAddTagsForAppManagedSpaces",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:AddTags"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
    "Condition" : {
        "StringEquals" : {
            "sagemaker:TaggingAction" : "CreateSpace"
        }
    }
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

Descrizione: politica del ruolo di servizio utilizzata da AWS ApiGateway all'interno dei AWS ServiceCatalog prodotti forniti dal portafoglio di prodotti Amazon SageMaker . Concede le autorizzazioni per una serie di servizi correlati, tra cui Lambda e altri.

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy è [una politica gestita AWS](#) .

Utilizzo di questa politica

Puoi collegarti

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 agosto 2023, 15:06 UTC
- Ora modificata: 01 agosto 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS CloudFormation interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati tra cui Lambda, ApiGateway e altri.

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy è [una](#) politica gestita AWS.

Utilizzo di questa politica

Puoi collegarti

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 agosto 2023, 15:06 UTC
- Ora modificata: 01 agosto 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
        }
    }
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

Descrizione: politica del ruolo di servizio utilizzata da AWS Lambda all'interno dei prodotti AWS ServiceCatalog forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a una serie di servizi correlati, tra cui Secrets Manager e altri.

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 agosto 2023, 15:05 UTC
- Ora modificata: 01 agosto 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerPipelinesIntegrations

Descrizione: questa Amazon Managed Policy concede le autorizzazioni comunemente necessarie per l'uso con le fasi di Callback e le fasi Lambda in Model Building Pipelines. SageMaker Viene aggiunto al AmazonSageMaker - ExecutionRole che può essere creato durante la configurazione di Studio. SageMaker Può anche essere associato a qualsiasi altro ruolo che verrà utilizzato per la creazione o l'esecuzione di pipeline.

AmazonSageMakerPipelinesIntegrations è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerPipelinesIntegrations ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 luglio 2021, 16:35 UTC
- Ora modificata: 17 febbraio 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon SageMaker tramite l'SDK AWS Management Console and.

AmazonSageMakerReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 13:07 UTC
- Ora modificata: 01 dicembre 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

Descrizione: politica del ruolo di servizio utilizzata da AWS ApiGateway all'interno dei AWS ServiceCatalog prodotti forniti dal portafoglio di prodotti Amazon SageMaker . Concede le autorizzazioni a una serie di servizi correlati, tra cui Logs e altri. CloudWatch

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy è [una politica gestita AWS](#) .

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 marzo 2022, 04:25 UTC

- Ora modificata: 25 marzo 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS CloudFormation interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, inclusi altri. SageMaker

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 marzo 2022, 04:26 UTC
- Ora modificata: 25 marzo 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
```

```
"sagemaker:CreateLineageGroupPolicy",
"sagemaker:CreateModel",
"sagemaker:CreateModelBiasJobDefinition",
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker:DeleteAction",
"sagemaker:DeleteAlgorithm",
"sagemaker:DeleteApp",
"sagemaker:DeleteAppImageConfig",
"sagemaker:DeleteArtifact",
"sagemaker:DeleteAssociation",
"sagemaker:DeleteCodeRepository",
"sagemaker:DeleteContext",
"sagemaker:DeleteDataQualityJobDefinition",
"sagemaker:DeleteDeviceFleet",
"sagemaker:DeleteDomain",
"sagemaker:DeleteEndpoint",
"sagemaker:DeleteEndpointConfig",
"sagemaker:DeleteExperiment",
"sagemaker:DeleteFeatureGroup",
"sagemaker:DeleteFlowDefinition",
"sagemaker:DeleteHumanLoop",
"sagemaker:DeleteHumanTaskUi",
"sagemaker:DeleteImage",
"sagemaker:DeleteImageVersion",
"sagemaker:DeleteLineageGroupPolicy",
"sagemaker:DeleteModel",
```

```
"sagemaker:DeleteModelBiasJobDefinition",
"sagemaker:DeleteModelExplainabilityJobDefinition",
"sagemaker:DeleteModelPackage",
"sagemaker:DeleteModelPackageGroup",
"sagemaker:DeleteModelPackageGroupPolicy",
"sagemaker:DeleteModelQualityJobDefinition",
"sagemaker:DeleteMonitoringSchedule",
"sagemaker:DeleteNotebookInstance",
"sagemaker:DeleteNotebookInstanceLifecycleConfig",
"sagemaker:DeletePipeline",
"sagemaker:DeleteProject",
"sagemaker:DeleteRecord",
"sagemaker:DeleteTags",
"sagemaker:DeleteTrial",
"sagemaker:DeleteTrialComponent",
"sagemaker:DeleteUserProfile",
"sagemaker:DeleteWorkforce",
"sagemaker:DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
```

```
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
```

```
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
```



```
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfiles",
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
"sagemaker:StopCompilationJob",
"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
```

```

        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
    ],
    "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS CodeBuild interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, tra cui CodePipeline, e altri. CodeBuild

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 marzo 2022, 04:27 UTC
- Ora modificata: 11 giugno 2024, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```

        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
    ],
    "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
},
{
    "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
    "Effect" : "Allow",
    "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
    "Effect" : "Allow",
    "Action" : [
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
    ],
    "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
    ]
},
{
    "Sid" : "AmazonSageMakerCodeBuildPassRolePermission",
    "Effect" : "Allow",
    "Action" : [

```

```

        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalogProductsExecutionRole"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "events.amazonaws.com",
                "codepipeline.amazonaws.com",
                "cloudformation.amazonaws.com",
                "codebuild.amazonaws.com",
                "sagemaker.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AmazonSageMakerCodeBuildLogPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs>DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",

```

```

        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
},
{
    "Sid" : "AmazonSageMakerCodeBuildS3Permission",
    "Effect" : "Allow",
    "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
    ]
},
{
    "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
    "Effect" : "Allow",
    "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",

```

```
"sagemaker:CreateAlgorithm",
"sagemaker:CreateApp",
"sagemaker:CreateAppImageConfig",
"sagemaker:CreateArtifact",
"sagemaker:CreateAutoMLJob",
"sagemaker:CreateCodeRepository",
"sagemaker:CreateCompilationJob",
"sagemaker:CreateContext",
"sagemaker:CreateDataQualityJobDefinition",
"sagemaker:CreateDeviceFleet",
"sagemaker:CreateDomain",
"sagemaker:CreateEdgePackagingJob",
"sagemaker:CreateEndpoint",
"sagemaker:CreateEndpointConfig",
"sagemaker:CreateExperiment",
"sagemaker:CreateFeatureGroup",
"sagemaker:CreateFlowDefinition",
"sagemaker:CreateHumanTaskUi",
"sagemaker:CreateHyperParameterTuningJob",
"sagemaker:CreateImage",
"sagemaker:CreateImageVersion",
"sagemaker:CreateInferenceRecommendationsJob",
"sagemaker:CreateLabelingJob",
"sagemaker:CreateLineageGroupPolicy",
"sagemaker:CreateModel",
"sagemaker:CreateModelBiasJobDefinition",
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
"sagemaker:CreateWorkforce",
```

```
"sagemaker:CreateWorkteam",
"sagemaker:DeleteAction",
"sagemaker:DeleteAlgorithm",
"sagemaker:DeleteApp",
"sagemaker:DeleteAppImageConfig",
"sagemaker:DeleteArtifact",
"sagemaker:DeleteAssociation",
"sagemaker:DeleteCodeRepository",
"sagemaker:DeleteContext",
"sagemaker:DeleteDataQualityJobDefinition",
"sagemaker:DeleteDeviceFleet",
"sagemaker:DeleteDomain",
"sagemaker:DeleteEndpoint",
"sagemaker:DeleteEndpointConfig",
"sagemaker:DeleteExperiment",
"sagemaker:DeleteFeatureGroup",
"sagemaker:DeleteFlowDefinition",
"sagemaker:DeleteHumanLoop",
"sagemaker:DeleteHumanTaskUi",
"sagemaker:DeleteImage",
"sagemaker:DeleteImageVersion",
"sagemaker:DeleteLineageGroupPolicy",
"sagemaker:DeleteModel",
"sagemaker:DeleteModelBiasJobDefinition",
"sagemaker:DeleteModelExplainabilityJobDefinition",
"sagemaker:DeleteModelPackage",
"sagemaker:DeleteModelPackageGroup",
"sagemaker:DeleteModelPackageGroupPolicy",
"sagemaker:DeleteModelQualityJobDefinition",
"sagemaker:DeleteMonitoringSchedule",
"sagemaker:DeleteNotebookInstance",
"sagemaker:DeleteNotebookInstanceLifecycleConfig",
"sagemaker:DeletePipeline",
"sagemaker:DeleteProject",
"sagemaker:DeleteRecord",
"sagemaker:DeleteTags",
"sagemaker:DeleteTrial",
"sagemaker:DeleteTrialComponent",
"sagemaker:DeleteUserProfile",
"sagemaker:DeleteWorkforce",
"sagemaker:DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
"sagemaker:DescribeAlgorithm",
```



```
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
"sagemaker:DescribeTrialComponent",
```

```
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
"sagemaker:ListLabelingJobsForWorkteam",
```

```
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfiles",
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
"sagemaker:StopCompilationJob",
```

```

"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
"sagemaker:UpdateModelPackage",
"sagemaker:UpdateMonitoringSchedule",
"sagemaker:UpdateNotebookInstance",
"sagemaker:UpdateNotebookInstanceLifecycleConfig",
"sagemaker:UpdatePipeline",
"sagemaker:UpdatePipelineExecution",
"sagemaker:UpdateProject",
"sagemaker:UpdateTrainingJob",
"sagemaker:UpdateTrial",
"sagemaker:UpdateTrialComponent",
"sagemaker:UpdateUserProfile",
"sagemaker:UpdateWorkforce",
"sagemaker:UpdateWorkteam"
],
"Resource" : [
  "arn:aws:sagemaker::*:endpoint/*",
  "arn:aws:sagemaker::*:endpoint-config/*",
  "arn:aws:sagemaker::*:model/*",
  "arn:aws:sagemaker::*:pipeline/*",
  "arn:aws:sagemaker::*:project/*",
  "arn:aws:sagemaker::*:model-package/*"
]

```

```

    ]
  },
  {
    "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:UseConnection"
    ],
    "Resource" : [
      "arn:aws:codestar-connections:*:*:connection/*"
    ],
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "aws:ResourceTag/sagemaker" : "true"
      }
    }
  },
  {
    "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
    "Effect" : "Allow",
    "Action" : [
      "codeconnections:UseConnection"
    ],
    "Resource" : [
      "arn:aws:codeconnections:*:*:connection/*"
    ],
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "aws:ResourceTag/sagemaker" : "true"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS CodePipeline interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, tra cui CodePipeline, e altri. CodeBuild

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 febbraio 2022, 09:53 UTC
- Ora modificata: 11 giugno 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```

    "Action" : [
      "cloudformation:CreateChangeSet",
      "cloudformation:CreateStack",
      "cloudformation:DescribeChangeSet",
      "cloudformation>DeleteChangeSet",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:ExecuteChangeSet",
      "cloudformation:SetStackPolicy",
      "cloudformation:UpdateStack"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
  },
  {
    "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:TagResource",
      "cloudformation:UntagResource"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "sagemaker:project-name"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonSageMakerCodePipelineS3Permission",
    "Effect" : "Allow",
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*:sagemaker-*"
    ]
  },
  {

```

```

    "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
    ]
},
{
    "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
    "Effect" : "Allow",
    "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
    ],
    "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
    ]
},
{
    "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
    "Effect" : "Allow",
    "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
    ],
    "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
},
{
    "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
    "Effect" : "Allow",
    "Action" : [
        "codestar-connections:UseConnection"
    ],
    "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*"
    ],
    "Condition" : {

```



```
    "StringEqualsIgnoreCase" : {
      "aws:ResourceTag/sagemaker" : "true"
    }
  },
  {
    "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
    "Effect" : "Allow",
    "Action" : [
      "codeconnections:UseConnection"
    ],
    "Resource" : [
      "arn:aws:codeconnections:*:*:connection/*"
    ],
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "aws:ResourceTag/sagemaker" : "true"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata dagli AWS CloudWatch Eventi all'interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, inclusi altri. CodePipeline

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 febbraio 2022, 09:53 UTC
- Ora modificata: 22 febbraio 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata da AWS Firehose nell'ambito dei prodotti AWS ServiceCatalog forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni per una serie di servizi correlati, tra cui Firehose e altri.

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 febbraio 2022, 09:54 UTC
- Ora modificata: 22 febbraio 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord",
      "firehose:PutRecordBatch"
    ],
    "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata da AWS Glue all'interno AWS ServiceCatalog dei prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a una serie di servizi correlati tra cui Glue, S3 e altri.

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 febbraio 2022, 09:51 UTC
- Ora modificata: 26 agosto 2022, 19:13 UTC

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

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Descrizione: politica del ruolo di servizio utilizzata da AWS Lambda all'interno dei prodotti AWS ServiceCatalog forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni per una serie di servizi correlati tra cui ECR, S3 e altri.

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 4 aprile 2022, 16:34 UTC
- Ora modificata: 11 giugno 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerLambdaECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr>DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaEventBridgePermission",
```



```

    "Effect" : "Allow",
    "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
    ]
},
{
    "Sid" : "AmazonSageMakerLambdaS3BucketPermission",
    "Effect" : "Allow",
    "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
    ]
},
{
    "Sid" : "AmazonSageMakerLambdaS3ObjectPermission",
    "Effect" : "Allow",
    "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
    ]
}

```

```
]
},
{
  "Sid" : "AmazonSageMakerLambdaSageMakerPermission",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddAssociation",
    "sagemaker:AddTags",
    "sagemaker:AssociateTrialComponent",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:BatchGetMetrics",
    "sagemaker:BatchGetRecord",
    "sagemaker:BatchPutMetrics",
    "sagemaker:CreateAction",
    "sagemaker:CreateAlgorithm",
    "sagemaker:CreateApp",
    "sagemaker:CreateAppImageConfig",
    "sagemaker:CreateArtifact",
    "sagemaker:CreateAutoMLJob",
    "sagemaker:CreateCodeRepository",
    "sagemaker:CreateCompilationJob",
    "sagemaker:CreateContext",
    "sagemaker:CreateDataQualityJobDefinition",
    "sagemaker:CreateDeviceFleet",
    "sagemaker:CreateDomain",
    "sagemaker:CreateEdgePackagingJob",
    "sagemaker:CreateEndpoint",
    "sagemaker:CreateEndpointConfig",
    "sagemaker:CreateExperiment",
    "sagemaker:CreateFeatureGroup",
    "sagemaker:CreateFlowDefinition",
    "sagemaker:CreateHumanTaskUi",
    "sagemaker:CreateHyperParameterTuningJob",
    "sagemaker:CreateImage",
    "sagemaker:CreateImageVersion",
    "sagemaker:CreateInferenceRecommendationsJob",
    "sagemaker:CreateLabelingJob",
    "sagemaker:CreateLineageGroupPolicy",
    "sagemaker:CreateModel",
    "sagemaker:CreateModelBiasJobDefinition",
    "sagemaker:CreateModelExplainabilityJobDefinition",
    "sagemaker:CreateModelPackage",
    "sagemaker:CreateModelPackageGroup",
    "sagemaker:CreateModelQualityJobDefinition",
```

```
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker:DeleteAction",
"sagemaker:DeleteAlgorithm",
"sagemaker:DeleteApp",
"sagemaker:DeleteAppImageConfig",
"sagemaker:DeleteArtifact",
"sagemaker:DeleteAssociation",
"sagemaker:DeleteCodeRepository",
"sagemaker:DeleteContext",
"sagemaker:DeleteDataQualityJobDefinition",
"sagemaker:DeleteDeviceFleet",
"sagemaker:DeleteDomain",
"sagemaker:DeleteEndpoint",
"sagemaker:DeleteEndpointConfig",
"sagemaker:DeleteExperiment",
"sagemaker:DeleteFeatureGroup",
"sagemaker:DeleteFlowDefinition",
"sagemaker:DeleteHumanLoop",
"sagemaker:DeleteHumanTaskUi",
"sagemaker:DeleteImage",
"sagemaker:DeleteImageVersion",
"sagemaker:DeleteLineageGroupPolicy",
"sagemaker:DeleteModel",
"sagemaker:DeleteModelBiasJobDefinition",
"sagemaker:DeleteModelExplainabilityJobDefinition",
"sagemaker:DeleteModelPackage",
"sagemaker:DeleteModelPackageGroup",
"sagemaker:DeleteModelPackageGroupPolicy",
"sagemaker:DeleteModelQualityJobDefinition",
"sagemaker:DeleteMonitoringSchedule",
```

```
"sagemaker:DeleteNotebookInstance",
"sagemaker:DeleteNotebookInstanceLifecycleConfig",
"sagemaker:DeletePipeline",
"sagemaker:DeleteProject",
"sagemaker:DeleteRecord",
"sagemaker:DeleteTags",
"sagemaker:DeleteTrial",
"sagemaker:DeleteTrialComponent",
"sagemaker:DeleteUserProfile",
"sagemaker:DeleteWorkforce",
"sagemaker:DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
```

```
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
```

```
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfiles",
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
```

```
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
"sagemaker:StopCompilationJob",
"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
"sagemaker:UpdateModelPackage",
"sagemaker:UpdateMonitoringSchedule",
"sagemaker:UpdateNotebookInstance",
"sagemaker:UpdateNotebookInstanceLifecycleConfig",
"sagemaker:UpdatePipeline",
"sagemaker:UpdatePipelineExecution",
"sagemaker:UpdateProject",
```

```

"sagemaker:UpdateTrainingJob",
"sagemaker:UpdateTrial",
"sagemaker:UpdateTrialComponent",
"sagemaker:UpdateUserProfile",
"sagemaker:UpdateWorkforce",
"sagemaker:UpdateWorkteam"
],
"Resource" : [
  "arn:aws:sagemaker:*:*:action/*",
  "arn:aws:sagemaker:*:*:algorithm/*",
  "arn:aws:sagemaker:*:*:app-image-config/*",
  "arn:aws:sagemaker:*:*:artifact/*",
  "arn:aws:sagemaker:*:*:automl-job/*",
  "arn:aws:sagemaker:*:*:code-repository/*",
  "arn:aws:sagemaker:*:*:compilation-job/*",
  "arn:aws:sagemaker:*:*:context/*",
  "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
  "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
  "arn:aws:sagemaker:*:*:device-fleet/*",
  "arn:aws:sagemaker:*:*:edge-packaging-job/*",
  "arn:aws:sagemaker:*:*:endpoint/*",
  "arn:aws:sagemaker:*:*:endpoint-config/*",
  "arn:aws:sagemaker:*:*:experiment/*",
  "arn:aws:sagemaker:*:*:experiment-trial/*",
  "arn:aws:sagemaker:*:*:experiment-trial-component/*",
  "arn:aws:sagemaker:*:*:feature-group/*",
  "arn:aws:sagemaker:*:*:human-loop/*",
  "arn:aws:sagemaker:*:*:human-task-ui/*",
  "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
  "arn:aws:sagemaker:*:*:image/*",
  "arn:aws:sagemaker:*:*:image-version/*/*",
  "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
  "arn:aws:sagemaker:*:*:labeling-job/*",
  "arn:aws:sagemaker:*:*:model/*",
  "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
  "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
  "arn:aws:sagemaker:*:*:model-package/*",
  "arn:aws:sagemaker:*:*:model-package-group/*",
  "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
  "arn:aws:sagemaker:*:*:monitoring-schedule/*",
  "arn:aws:sagemaker:*:*:notebook-instance/*",
  "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
  "arn:aws:sagemaker:*:*:pipeline/*",
  "arn:aws:sagemaker:*:*:pipeline/*/execution/*",

```



```

        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
    ]
},
{
    "Sid" : "AmazonSageMakerLambdaPassRolePermission",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
    ]
},
{
    "Sid" : "AmazonSageMakerLambdaLogPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs>DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}

```

```
    },
    {
      "Sid" : "AmazonSageMakerLambdaCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/sagemaker-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:project-name" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSecurityLakeAdministrator

Descrizione: fornisce l'accesso completo ad Amazon Security Lake e ai servizi correlati necessari per amministrare Security Lake.

AmazonSecurityLakeAdministrator è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSecurityLakeAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2023, 22:04 UTC

- Ora modificata: 23 febbraio 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSecurityLakeMetastoreManager

Descrizione: Policy per Amazon SecurityLake meta store manager lambda che consente l'accesso a cloudwatch, S3, Glue e SQS.

AmazonSecurityLakeMetastoreManager [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonSecurityLakeMetastoreManager ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 23 gennaio 2024, 15:26 UTC
- Ora modificata: 01 aprile 2024, 20:04 UTC

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

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "AllowToReadFromSqs",
    "Effect" : "Allow",
    "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes"
    ],
    "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "AllowMetaDataReadWrite",
    "Effect" : "Allow",
    "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
}

```



```
    }
  },
  {
    "Sid" : "AllowMetaDataCleanup",
    "Effect" : "Allow",
    "Action" : [
      "s3:DeleteObject"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
      "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSecurityLakePermissionsBoundary

Descrizione: Amazon Security Lake crea ruoli IAM per fonti personalizzate di terze parti per scrivere dati su un data lake e per gli abbonati di terze parti per utilizzare i dati da un data lake e utilizza questa politica durante la creazione di questi ruoli per definire i limiti delle loro autorizzazioni.

AmazonSecurityLakePermissionsBoundary [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonSecurityLakePermissionsBoundary ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2022, 14:11 UTC
- Ora modificata: 14 maggio 2024, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsForSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs>DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ]
    }
  ],
```

```

    "Resource" : "*"
  },
  {
    "Sid" : "DenyActionsForSecurityLake",
    "Effect" : "Deny",
    "NotAction" : [
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:ListBucket",
      "s3:ListBucketVersions",
      "s3:PutObject",
      "s3:GetBucketLocation",
      "kms:Decrypt",
      "kms:GenerateDataKey",
      "sqs:ReceiveMessage",
      "sqs:ChangeMessageVisibility",
      "sqs:DeleteMessage",
      "sqs:GetQueueUrl",
      "sqs:SendMessage",
      "sqs:GetQueueAttributes",
      "sqs:ListQueues"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DenyActionsNotOnSecurityLakeBucket",
    "Effect" : "Deny",
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:ListBucket",
      "s3:ListBucketVersions",
      "s3:PutObject",
      "s3:GetBucketLocation"
    ],
    "NotResource" : [
      "arn:aws:s3::aws-security-data-lake*"
    ]
  },
  {
    "Sid" : "DenyActionsNotOnSecurityLakeSQS",
    "Effect" : "Deny",
    "Action" : [
      "sqs:ReceiveMessage",

```

```

        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
    ],
    "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
},
{
    "Sid" : "DenyActionsNotOnSecurityLakeKMSS3SQS",
    "Effect" : "Deny",
    "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringNotLike" : {
            "kms:ViaService" : [
                "s3.*.amazonaws.com",
                "sqs.*.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3",
    "Effect" : "Deny",
    "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringNotLikeIfExists" : {
            "kms:EncryptionContext:aws:s3:arn" : [
                "arn:aws:s3:::aws-security-data-lake*"
            ]
        }
    }
}
}

```

```
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:sqs:arn" : [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSESFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SES tramite AWS Management Console.

AmazonSESFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSESFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSESReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon SES tramite AWS Management Console.

AmazonSESReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSESReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 14 maggio 2024, 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSESServiceRolePolicy

Descrizione: consente a SES di pubblicare i parametri CloudWatch di monitoraggio di Amazon Basic per conto delle tue risorse SES

AmazonSESServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 maggio 2024, 16:02 UTC
- Ora modificata: 21 maggio 2024, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricDataToSESCloudWatchNamespaces",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "AWS/SES",
            "AWS/SES/MailManager",
            "AWS/SES/Addons"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSNSFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SNS tramite AWS Management Console

AmazonSNSFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSNSFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSNSReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon SNS tramite. AWS Management Console

AmazonSNSReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSNSReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSNSRole

Descrizione: policy predefinita per il ruolo del servizio Amazon SNS.

AmazonSNSRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSNSRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Action" : [
  "logs:CreateLogGroup",
  "logs:CreateLogStream",
  "logs:PutLogEvents",
  "logs:PutMetricFilter",
  "logs:PutRetentionPolicy"
],
"Resource" : [
  "*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSQSFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SQS tramite AWS Management Console

AmazonSQSFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSQSFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSQSReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon SQS tramite AWS Management Console

AmazonSQSReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSQSReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 24 maggio 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMAutomationApproverAccess

Descrizione: fornisce l'accesso per visualizzare le esecuzioni di automazione e inviare le decisioni di approvazione all'automazione in attesa di approvazione

AmazonSSMAutomationApproverAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSSMAutomationApproverAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 agosto 2017, 23:07 UTC
- Ora modificata: 07 agosto 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
"Effect" : "Allow",
"Action" : [
  "ssm:DescribeAutomationExecutions",
  "ssm:GetAutomationExecution",
  "ssm:SendAutomationSignal"
],
"Resource" : [
  "*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMAutomationRole

Descrizione: fornisce le autorizzazioni al servizio EC2 Automation per eseguire le attività definite nei documenti di automazione

AmazonSSMAutomationRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSSMAutomationRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 dicembre 2016, 22:09 UTC
- Ora modificata: 24 luglio 2017, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMDirectoryServiceAccess

Descrizione: questo criterio consente all'agente SSM di accedere al Directory Service per conto del cliente per l'aggiunta al dominio dell'istanza gestita.

AmazonSSMDirectoryServiceAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonSSMDirectoryServiceAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 marzo 2019, 17:44 UTC
- Ora modificata: 15 marzo 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SSM.

AmazonSSMFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSSMFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 maggio 2015, 17:39 UTC
- Ora modificata: 20 novembre 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMMaintenanceWindowRole

Descrizione: ruolo di servizio da utilizzare per la finestra di manutenzione di EC2

AmazonSSMMaintenanceWindowRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSSMMaintenanceWindowRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2016, 15:57 UTC
- Ora modificata: 27 luglio 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [  
        "*"   
    ]  
  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMManagedEC2InstanceDefaultPolicy

Descrizione: questa policy abilita la funzionalità AWS Systems Manager sulle istanze EC2.

AmazonSSMManagedEC2InstanceDefaultPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSSMManagedEC2InstanceDefaultPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 agosto 2022, 20:54 UTC
- Ora modificata: 30 agosto 2022, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMManagedInstanceCore

Descrizione: la policy per il ruolo di Amazon EC2 per abilitare le funzionalità principali del servizio AWS Systems Manager.

AmazonSSMManagedInstanceCore è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSSMManagedInstanceCore ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 marzo 2019, 17:22 UTC
- Ora modificata: 23 maggio 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMPatchAssociation

Descrizione: Fornisci l'accesso alle istanze secondarie per le operazioni di associazione delle patch.

AmazonSSMPatchAssociation è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSSMPatchAssociation ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 maggio 2020, 16:00 UTC
- Ora modificata: 13 maggio 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon SSM.

AmazonSSMReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSSMReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 maggio 2015, 17:44 UTC
- Ora modificata: 29 maggio 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSSMServiceRolePolicy

Descrizione: Fornisce l'accesso alle AWS risorse gestite o utilizzate da Amazon SSM

AmazonSSMServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 novembre 2017, 19:20 UTC
- Ora modificata: 14 settembre 2022, 19:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
```

```

        "*"
    ],
},
{
    "Effect" : "Allow",
    "Action" : [
        "lambda:InvokeFunction"
    ],
    "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
    ],
    "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "resource-groups: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" : "*"
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonSumerianFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Sumerian.

AmazonSumerianFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonSumerianFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 aprile 2018, 20:14 UTC
- Ora modificata: 24 aprile 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "sumerian:*"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTextractFullAccess

Descrizione: Accesso a tutte le API Amazon Textract

AmazonTextractFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonTextractFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 19:07 UTC
- Ora modificata: 28 novembre 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTextractServiceRole

Descrizione: consente a Textract di chiamare AWS i servizi per tuo conto.

AmazonTextractServiceRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonTextractServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio

- Ora di creazione: 28 novembre 2018, 19:12 UTC
- Ora modificata: 28 novembre 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTimestreamConsoleFullAccess

Descrizione: fornisce l'accesso completo per gestire Amazon Timestream utilizzando. AWS Management Console Tieni presente che questa politica concede anche le autorizzazioni per

determinate operazioni KMS e operazioni per la gestione delle query salvate. Se utilizzi la CMK gestita dal cliente, consulta la documentazione per le autorizzazioni aggiuntive necessarie.

AmazonTimestreamConsoleFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonTimestreamConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2020, 21:47 UTC
- Ora modificata: 01 febbraio 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTimestreamFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Timestream. Tieni presente che questa politica concede anche determinati accessi operativi KMS. Se utilizzi la CMK gestita dal cliente, consulta la documentazione per le autorizzazioni aggiuntive necessarie.

AmazonTimestreamFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonTimestreamFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2020, 21:47 UTC
- Ora modificata: 26 novembre 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTimestreamInfluxDBFullAccess

Descrizione: fornisce l'accesso amministrativo completo per creare, aggiornare, eliminare ed elencare istanze Amazon Timestream InfluxDB e creare ed elencare gruppi di parametri. Consulta la documentazione per le autorizzazioni aggiuntive necessarie.

AmazonTimestreamInfluxDBFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonTimestreamInfluxDBFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 marzo 2024, 22:53 UTC
- Ora modificata: 14 marzo 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:::*"
    ]
  }
]

```



```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTimestreamInfluxDBServiceRolePolicy

Descrizione: fornisce l'accesso amministrativo completo per creare, aggiornare, eliminare ed elencare istanze Amazon Timestream InfluxDB e creare ed elencare gruppi di parametri. Consulta la documentazione per le autorizzazioni aggiuntive necessarie.

AmazonTimestreamInfluxDBServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 marzo 2024, 18:53 UTC
- Ora modificata: 14 marzo 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
    }
  }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTimestreamReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Timestream. La policy fornisce inoltre l'autorizzazione per annullare qualsiasi query in esecuzione. Se utilizzi la CMK gestita dal cliente, consulta la documentazione per le autorizzazioni aggiuntive necessarie.

AmazonTimestreamReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonTimestreamReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 30 settembre 2020, 21:47 UTC
- Ora modificata: 5 giugno 2024, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonTimestreamReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks",
        "timestream:DescribeAccountSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTranscribeFullAccess

Descrizione: Fornisce accesso completo alle operazioni di Amazon Transcribe

AmazonTranscribeFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonTranscribeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 aprile 2018, 16:06 UTC
- Ora modificata: 4 aprile 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "transcribe:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*transcribe*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonTranscribeReadOnlyAccess

Descrizione: fornisce l'accesso alle operazioni di sola lettura per Amazon Transcribe

AmazonTranscribeReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonTranscribeReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 aprile 2018, 16:05 UTC

- Ora modificata: 4 aprile 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

Descrizione: fornisce l'accesso per creare interfacce di rete e collegarle a risorse tra più account

AmazonVPCCrossAccountNetworkInterfaceOperations è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonVPCCrossAccountNetworkInterfaceOperations ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 luglio 2017, 20:47 UTC
- Ora modificata: 25 settembre 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonVPCFullAccess

Descrizione: fornisce l'accesso completo ad Amazon VPC tramite AWS Management Console.

AmazonVPCFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonVPCFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 08 febbraio 2024, 16:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Descrizione: fornisce le autorizzazioni per descrivere AWS le risorse, eseguire Network Access Analyzer e creare o eliminare tag su Network Insights Access Scope e Network Insights Access Scope Analysis.

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonVPCNetworkAccessAnalyzerFullAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 giugno 2023, 22:56 UTC
- Ora modificata: 15 maggio 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```



```

},
{
  "Sid" : "EC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInsightsAccessScope",
    "ec2:DeleteNetworkInsightsAccessScope",
    "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
    "ec2:DescribeNetworkInsightsAccessScopes",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
    "ec2:GetNetworkInsightsAccessScopeContent",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "ec2:StartNetworkInsightsAccessScopeAnalysis"
  ],
  "Resource" : "*"
},

```

```

{
  "Sid" : "EC2TagsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:network-insights-access-scope/*",
    "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
  ]
},
{
  "Sid" : "ElasticloadbalancingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GlobalacceleratorPermissions",
  "Effect" : "Allow",
  "Action" : [
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners"
  ],
  "Resource" : "*"
},
{
  "Sid" : "NetworkFirewallPermissions",
  "Effect" : "Allow",

```

```

    "Action" : [
      "network-firewall:DescribeFirewall",
      "network-firewall:DescribeFirewallPolicy",
      "network-firewall:DescribeResourcePolicy",
      "network-firewall:DescribeRuleGroup",
      "network-firewall:ListFirewallPolicies",
      "network-firewall:ListFirewalls",
      "network-firewall:ListRuleGroups"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ResourceGroupsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:ListGroupResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TagsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TirosPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tiros:CreateQuery",
      "tiros:GetQueryAnswer"
    ],
    "Resource" : "*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Descrizione: fornisce le autorizzazioni per descrivere AWS le risorse, eseguire Reachability Analyzer e creare o eliminare tag su Network Insights Path e Network Insights Analysis.

AmazonVPCReachabilityAnalyzerFullAccessPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonVPCReachabilityAnalyzerFullAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 giugno 2023, 20:12 UTC
- Ora modificata: 15 maggio 2024, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Effect" : "Allow",
"Action" : [
  "directconnect:DescribeConnections",
  "directconnect:DescribeDirectConnectGatewayAssociations",
  "directconnect:DescribeDirectConnectGatewayAttachments",
  "directconnect:DescribeDirectConnectGateways",
  "directconnect:DescribeVirtualGateways",
  "directconnect:DescribeVirtualInterfaces"
],
"Resource" : "*"
},
{
  "Sid" : "EC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInsightsPath",
    "ec2:DeleteNetworkInsightsAnalysis",
    "ec2:DeleteNetworkInsightsPath",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInsightsAnalyses",
    "ec2:DescribeNetworkInsightsPaths",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
```

```

        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
    ],
    "Resource" : "*"
},
{
    "Sid" : "EC2TagsPermissions",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags",
        "ec2>DeleteTags"
    ],
    "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
    ]
},
{
    "Sid" : "ElasticloadbalancingPermissions",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
    ],
    "Resource" : "*"
},
{
    "Sid" : "GlobalacceleratorPermissions",
    "Effect" : "Allow",
    "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",

```

```
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
    ],
    "Resource" : "*"
},
{
    "Sid" : "NetworkFirewallPermissions",
    "Effect" : "Allow",
    "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
    ],
    "Resource" : "*"
},
{
    "Sid" : "TiroPermissions",
    "Effect" : "Allow",
    "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Descrizione: questa policy è allegata al ruolo

IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Questo ruolo viene distribuito agli account dei membri di un'organizzazione quando l'account di gestione consente l'accesso affidabile per Reachability Analyzer. Fornisce le autorizzazioni per visualizzare le risorse di tutta l'organizzazione utilizzando la console Reachability Analyzer.

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonVPCReachabilityAnalyzerPathComponentReadPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 maggio 2023, 20:38 UTC
- Ora modificata: 01 maggio 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
"Effect" : "Allow",
"Action" : [
  "network-firewall:Describe*",
  "network-firewall:List*"
],
"Resource" : "*"
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonVPCReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon VPC tramite AWS Management Console

AmazonVPCReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonVPCReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 08 febbraio 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkDocsFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon WorkDocs tramite AWS Management Console

AmazonWorkDocsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonWorkDocsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2020, 23:05 UTC
- Ora modificata: 16 aprile 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkDocsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon WorkDocs tramite AWS Management Console

AmazonWorkDocsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonWorkDocsReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 gennaio 2020, 23:49 UTC
- Ora modificata: 08 gennaio 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkMailEventsServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon WorkMail Events

AmazonWorkMailEventsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 aprile 2019, 16:52 UTC
- Ora modificata: 16 aprile 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkMailFullAccess

Descrizione: Fornisce accesso completo ai metadati KMS WorkMail, Directory Service, SES, EC2 e accesso in lettura ai metadati KMS.

AmazonWorkMailFullAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonWorkMailFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 21 dicembre 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}

```

```
}  
  }  
    }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkMailMessageFlowFullAccess

Descrizione: accesso completo alle API WorkMail Message Flow

AmazonWorkMailMessageFlowFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonWorkMailMessageFlowFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 febbraio 2021, 11:08 UTC
- Ora modificata: 11 febbraio 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkMailMessageFlowReadOnlyAccess

Descrizione: accesso in sola lettura ai WorkMail messaggi per l' GetRawMessageContent API

AmazonWorkMailMessageFlowReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonWorkMailMessageFlowReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 gennaio 2021, 12:40 UTC
- Ora modificata: 28 gennaio 2021, 12:40 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkMailReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a WorkMail e SES.

AmazonWorkMailReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonWorkMailReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 25 luglio 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkSpacesAdmin

Descrizione: fornisce l'accesso alle azioni WorkSpaces amministrative di Amazon tramite AWS SDK e CLI.

AmazonWorkSpacesAdmin è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonWorkSpacesAdmin ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 settembre 2015, 22:21 UTC
- Ora modificata: 03 agosto 2023, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkSpacesApplicationManagerAdminAccess

Descrizione: fornisce l'accesso di amministratore per il pacchetto di un'applicazione in Amazon WorkSpaces Application Manager.

AmazonWorkSpacesApplicationManagerAdminAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonWorkSpacesApplicationManagerAdminAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 14:03 UTC
- Ora modificata: 9 aprile 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
    "Action" : "wam:AuthenticatePackager",
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkspacesPCAAccess

Descrizione: questa policy gestita fornisce l'accesso amministrativo completo alle risorse CA private di AWS Certificate Manager presenti nell'utente Account AWS per l'autenticazione basata su certificati.

AmazonWorkspacesPCAAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AmazonWorkspacesPCAAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 08 novembre 2022, 00:25 UTC
- Ora modificata: 08 novembre 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkSpacesSelfServiceAccess

Descrizione: Fornisce l'accesso al servizio di WorkSpaces backend Amazon per eseguire azioni self-service di Workspace

AmazonWorkSpacesSelfServiceAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AmazonWorkSpacesSelfServiceAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2019, 19:22 UTC
- Ora modificata: 27 giugno 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkSpacesServiceAccess

Descrizione: fornisce all'account del cliente l'accesso al AWS WorkSpaces servizio per l'avvio di un Workspace.

AmazonWorkSpacesServiceAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonWorkSpacesServiceAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2019, 19:19 UTC
- Ora modificata: 18 marzo 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkSpacesWebReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon WorkSpaces Web e alle sue dipendenze tramite SDK e AWS Management Console CLI.

AmazonWorkSpacesWebReadOnly è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmazonWorkSpacesWebReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2021, 14:20 UTC
- Ora modificata: 02 novembre 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonWorkSpacesWebServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon WorkSpaces Web

AmazonWorkSpacesWebServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 novembre 2021, 13:15 UTC
- Ora modificata: 15 dicembre 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonZocaloFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Zocalo.

AmazonZocaloFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonZocaloFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmazonZocaloReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon Zocalo

AmazonZocaloReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AmazonZocaloReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AmplifyBackendDeployFullAccess

Descrizione: Fornisce le autorizzazioni di accesso completo ad Amplify per distribuire le risorse di backend Amplify (AWS AppSyncAmazon Cognito, Amazon S3 e altri servizi correlati) tramite il Development Kit (CDK) Cloud AWS AWS

AmplifyBackendDeployFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AmplifyBackendDeployFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 ottobre 2023, 21:32 UTC
- Ora modificata: 31 maggio 2024, 15:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation>DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
```

```

    "Action" : [
      "appsync:GetSchemaCreationStatus",
      "appsync:StartSchemaCreation",
      "appsync:UpdateResolver",
      "appsync:ListFunctions",
      "appsync:UpdateFunction",
      "appsync:UpdateApiKey"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AmplifyHotSwappableFunctionResource",
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction",
      "lambda:UpdateFunctionCode",
      "lambda:GetFunction",
      "lambda:UpdateFunctionConfiguration"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:amplify-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AmplifySchema",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3::*:amplify*",
      "arn:aws:s3::*:cdk-*--assets-*-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }

```

```

    }
  },
  {
    "Sid" : "CDKDeploy",
    "Effect" : "Allow",
    "Action" : [
      "sts:AssumeRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
      "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
      "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
      "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AmplifySSM",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParametersByPath",
      "ssm:GetParameters",
      "ssm:GetParameter"
    ],
    "Resource" : [
      "arn:aws:ssm::*:parameter/amplify/*",
      "arn:aws:ssm::*:parameter/cdk-bootstrap/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AmplifyModifySSMParam",
    "Effect" : "Allow",
    "Action" : [
      "ssm:PutParameter",
      "ssm>DeleteParameter",

```



```

    "ssm:DeleteParameters"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AmplifyDiscoverRDSVpcConfig",
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBProxies",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "ec2:DescribeSubnets",
    "rds:DescribeDBSubnetGroups"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:db:*",
    "arn:aws:rds:*:*:cluster:*",
    "arn:aws:rds:*:*:db-proxy:*",
    "arn:aws:rds:*:*:subgrp:*",
    "arn:aws:ec2:*:*:subnet/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

APIGatewayServiceRolePolicy

Descrizione: consente ad API Gateway di gestire AWS le risorse associate per conto del cliente.

APIGatewayServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 ottobre 2017, 17:23 UTC
- Ora modificata: 12 luglio 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AppIntegrationsServiceLinkedRolePolicy

Descrizione: consente di AppIntegrations gestire AppFlow le risorse e pubblicare i dati CloudWatch metrici per tuo conto.

AppIntegrationsServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 settembre 2022, 19:42 UTC
- Ora modificata: 30 settembre 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ApplicationAutoScalingForAmazonAppStreamAccess

Descrizione: politica per abilitare l'autoscaling delle applicazioni per Amazon AppStream

ApplicationAutoScalingForAmazonAppStreamAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti ApplicationAutoScalingForAmazonAppStreamAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2017, 21:39 UTC
- Ora modificata: 6 febbraio 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite dalla funzionalità di esportazione continua di Application Discovery Service

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 09 agosto 2018, 20:22 UTC
- Ora modificata: 13 agosto 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AppRunnerNetworkingServiceRolePolicy

Descrizione: consente alla AWS AppRunner rete di gestire AWS le risorse correlate per tuo conto.

AppRunnerNetworkingServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 gennaio 2022, 21:02 UTC
- Ora modificata: 12 gennaio 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AppRunnerServiceRolePolicy

Descrizione: consente di AWS AppRunner gestire AWS le risorse correlate per tuo conto.

AppRunnerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 maggio 2021, 19:15 UTC
- Ora modificata: 14 maggio 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AutoScalingConsoleFullAccess

Descrizione: Fornisce l'accesso completo a Auto Scaling tramite. AWS Management Console

AutoScalingConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AutoScalingConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2017, 19:43 UTC
- Ora modificata: 6 febbraio 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
}
```

```
}  
  }  
] }  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AutoScalingConsoleReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura all'Auto Scaling tramite. AWS Management Console

AutoScalingConsoleReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AutoScalingConsoleReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2017, 19:48 UTC
- Ora modificata: 12 gennaio 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AutoScalingFullAccess

Descrizione: Fornisce l'accesso completo all'Auto Scaling.

AutoScalingFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AutoScalingFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2017, 19:31 UTC
- Ora modificata: 6 febbraio 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AutoScalingNotificationAccessRole

Descrizione: criterio predefinito per il ruolo del servizio AutoScaling Notification Access.

AutoScalingNotificationAccessRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AutoScalingNotificationAccessRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AutoScalingReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura all'Auto Scaling.

AutoScalingReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AutoScalingReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2017, 19:39 UTC
- Ora modificata: 12 gennaio 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AutoScalingServiceRolePolicy

Descrizione: Consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Auto Scaling

AutoScalingServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 8 gennaio 2018, 23:10 UTC
- Ora modificata: 29 febbraio 2024, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWS_ConfigRole

Descrizione: criterio predefinito per il AWS ruolo del servizio Config. Fornisce le autorizzazioni necessarie a AWS Config per tenere traccia delle modifiche alle AWS risorse.

AWS_ConfigRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWS_ConfigRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 15 settembre 2020, 20:30 UTC

- Ora modificata: 22 febbraio 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Versione della politica

Versione della politica: v30 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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",
"finespace:GetEnvironment",
"finespace: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:GetFirmwareTask",
"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/*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAccountActivityAccess

Descrizione: consente agli utenti di accedere alla pagina Attività dell'account.

AWSAccountActivityAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAccountActivityAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 07 marzo 2023, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAccountManagementFullAccess

Descrizione: fornisce l'accesso completo alla gestione degli AWS account.

AWSAccountManagementFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAccountManagementFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2021, 23:20 UTC
- Ora modificata: 30 settembre 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAccountManagementReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura alla gestione degli account AWS

AWSAccountManagementReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAccountManagementReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2021, 23:29 UTC
- Ora modificata: 30 settembre 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAccountUsageReportAccess

Descrizione: consente agli utenti di accedere alla pagina del rapporto sull'utilizzo dell'account.

AWSAccountUsageReportAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAccountUsageReportAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
{
  "Effect" : "Allow",
  "Action" : [
    "aws-portal:ViewUsage"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAgentlessDiscoveryService

Descrizione: fornisce l'accesso al Discovery Agentless Connector per la registrazione con AWS Application Discovery Service.

AWSAgentlessDiscoveryService è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAgentlessDiscoveryService ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 agosto 2016, 01:35 UTC
- Ora modificata: 24 febbraio 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppFabricFullAccess

Descrizione: fornisce l'accesso completo al AWS AppFabric servizio e l'accesso in sola lettura ai servizi dipendenti come S3, Kinesis, KMS.

AWSAppFabricFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSAppFabricFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2023, 19:51 UTC
- Ora modificata: 27 giugno 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
]
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppFabricReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS AppFabric

AWSAppFabricReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppFabricReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 27 giugno 2023, 19:52 UTC
- Ora modificata: 27 giugno 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppFabricServiceRolePolicy

Descrizione: fornisce AppFabric l'accesso alle AWS risorse per tuo conto

AWSAppFabricServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 giugno 2023, 21:07 UTC
- Ora modificata: 26 giugno 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

Descrizione: Politica che concede le autorizzazioni ad Application Auto Scaling per accedere e. AppStream CloudWatch

AWSApplicationAutoscalingAppStreamFleetPolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 ottobre 2017, 19:04 UTC
- Ora modificata: 20 ottobre 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingCassandraTablePolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere a Cassandra e. CloudWatch

AWSApplicationAutoscalingCassandraTablePolicy [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 marzo 2020, 22:49 UTC
- Ora modificata: 18 marzo 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere a Comprehend and. CloudWatch

AWSApplicationAutoscalingComprehendEndpointPolicy [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 novembre 2019, 18:39 UTC
- Ora modificata: 14 novembre 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoScalingCustomResourcePolicy

Descrizione: Policy che concede le autorizzazioni ad Application Auto Scaling per accedere ad CloudWatch APIGateway e per il ridimensionamento personalizzato delle risorse

AWSApplicationAutoScalingCustomResourcePolicy è una [AWS politica](#) gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 4 giugno 2018, 23:22 UTC
- Ora modificata: 04 giugno 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "execute-api:Invoke",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a DynamoDB e. CloudWatch

AWSApplicationAutoscalingDynamoDBTablePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 ottobre 2017, 21:34 UTC
- Ora modificata: 20 ottobre 2017, 21:34 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a EC2 Spot Fleet e. CloudWatch

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 25 ottobre 2017, 18:23 UTC
- Ora modificata: 25 ottobre 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingECSServicePolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a EC2 Container Service e. CloudWatch

AWSApplicationAutoscalingECSServicePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 25 ottobre 2017, 23:53 UTC
- Ora modificata: 25 ottobre 2017, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingElastiCacheRGPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere ad Amazon e Amazon ElastiCache . CloudWatch

AWSApplicationAutoscalingElastiCacheRGPolicy è [una politica gestita AWS](#) .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 agosto 2021, 23:41 UTC
- Ora modificata: 17 agosto 2021, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElasticCacheRGPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  ]
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a Elastic Map Reduce e. CloudWatch

AWSApplicationAutoscalingEMRInstanceGroupPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 ottobre 2017, 00:57 UTC
- Ora modificata: 26 ottobre 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingKafkaClusterPolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a Managed Streaming for Apache Kafka e. CloudWatch

AWSApplicationAutoscalingKafkaClusterPolicy è una [AWS politica](#) gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 agosto 2020, 18:36 UTC
- Ora modificata: 24 agosto 2020, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a Lambda e. CloudWatch

AWSApplicationAutoscalingLambdaConcurrencyPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 ottobre 2019, 20:04 UTC
- Ora modificata: 21 ottobre 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:PutProvisionedConcurrencyConfig",
      "lambda:GetProvisionedConcurrencyConfig",
      "lambda>DeleteProvisionedConcurrencyConfig",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere ad Amazon Neptune e Amazon. CloudWatch

AWSApplicationAutoscalingNeptuneClusterPolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 2 settembre 2021, 21:14 UTC

- Ora modificata: 2 settembre 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingRDSClusterPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere a RDS e. CloudWatch

AWSApplicationAutoscalingRDSClusterPolicy [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 ottobre 2017, 17:46 UTC
- Ora modificata: 07 agosto 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

Descrizione: Politica che concede le autorizzazioni ad Application Auto Scaling per accedere e. SageMaker CloudWatch

AWSApplicationAutoscalingSageMakerEndpointPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 6 febbraio 2018, 19:58 UTC
- Ora modificata: 13 novembre 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    ]
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationDiscoveryAgentAccess

Descrizione: fornisce l'accesso al Discovery Agent per la registrazione con AWS Application Discovery Service.

AWSApplicationDiscoveryAgentAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationDiscoveryAgentAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2016, 21:38 UTC
- Ora modificata: 24 febbraio 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

Descrizione: consente a Application Discovery Service Agentless Collector di aggiornare, registrare e comunicare automaticamente con Application Discovery Service

AWSApplicationDiscoveryAgentlessCollectorAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti `AWSApplicationDiscoveryAgentlessCollectorAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 16 agosto 2022, 21:00 UTC
- Ora modificata: 16 agosto 2022, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"   
  }  
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationDiscoveryServiceFullAccess

Descrizione: Fornisce l'accesso completo alla visualizzazione e all'etichettatura degli elementi di configurazione gestiti dall' AWS Application Discovery Service

AWSApplicationDiscoveryServiceFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSAApplicationDiscoveryServiceFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2016, 21:30 UTC
- Ora modificata: 19 giugno 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationAgentInstallationPolicy

Descrizione: questa politica consente di installare il AWS Replication Agent, che viene utilizzato con AWS Application Migration Service (MGN) per migrare server esterni verso. AWS Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante l'installazione del Replication Agent. AWS

AWSApplicationMigrationAgentInstallationPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationAgentInstallationPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 giugno 2022, 07:51 UTC
- Ora modificata: 20 settembre 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationAgentPolicy

Descrizione: questa policy consente l'installazione e l'utilizzo del AWS Replication Agent, utilizzato con AWS Application Migration Service (MGN) per migrare server esterni verso AWS. AWS Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante l'installazione del Replication Agent. AWS

AWSApplicationMigrationAgentPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationAgentPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 aprile 2021, 07:00 UTC
- Ora modificata: 20 settembre 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationAgentPolicy_v2

Descrizione: questa policy consente di utilizzare il AWS Replication Agent, utilizzato con AWS Application Migration Service (MGN) per migrare server esterni verso AWS. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

AWSApplicationMigrationAgentPolicy_v2 è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationAgentPolicy_v2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 giugno 2022, 14:14 UTC
- Ora modificata: 06 giugno 2022, 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationConversionServerPolicy

Descrizione: questa policy consente al server di conversione di Application Migration Service (MGN), che sono istanze EC2 lanciate da Application Migration Service, di comunicare con il servizio MGN. Un ruolo IAM con questa policy viene allegato (come profilo di istanza EC2) da MGN ai server di conversione MGN, che vengono avviati e terminati automaticamente da MGN, quando necessario. Non è consigliabile collegare questa policy ai propri utenti o ruoli IAM. I server di conversione MGN vengono utilizzati da Application Migration Service quando gli utenti scelgono di avviare istanze Test o Cutover utilizzando la console MGN, la CLI o l'API.

AWSApplicationMigrationConversionServerPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationConversionServerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 07 aprile 2021, 06:48 UTC
- Ora modificata: 07 aprile 2021, 06:48 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationEC2Access

Descrizione: questa policy fornisce le operazioni Amazon EC2 necessarie per utilizzare Application Migration Service (MGN) per avviare i server migrati come istanze EC2. Allega questa policy ai tuoi utenti o ruoli IAM.

AWSApplicationMigrationEC2Access è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationEC2Access ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 07 aprile 2021, 07:05 UTC
- Ora modificata: 06 febbraio 2023, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationFullAccess

Descrizione: questa policy fornisce le autorizzazioni per tutte le API pubbliche di AWS Application Migration Service (MGN), nonché le autorizzazioni per leggere le informazioni chiave KMS. Allega questa policy ai tuoi utenti o ruoli IAM.

AWSApplicationMigrationFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 7 aprile 2021, 06:56 UTC
- Ora modificata: 19 maggio 2024, 08:30 UTC

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

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
```

```

        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
    ],
    "Resource" : "*"
},
{
    "Sid" : "VisualEditor3",
    "Effect" : "Allow",
    "Action" : "license-manager:ListLicenseConfigurations",
    "Resource" : "*"
},
{
    "Sid" : "VisualEditor4",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
},
{
    "Sid" : "VisualEditor5",
    "Effect" : "Allow",
    "Action" : "iam:ListInstanceProfiles",
    "Resource" : "*"
},
{
    "Sid" : "VisualEditor6",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
    ]
}

```

```
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "VisualEditor7",
    "Effect" : "Allow",
    "Action" : [
      "drs:DescribeSourceServers"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "VisualEditor8",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      },
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Sid" : "VisualEditor9",
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListCommandInvocations"
    ],
    "Resource" : "*"
  },
  ],
```

```

{
  "Sid" : "VisualEditor10",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeInstanceInformation",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "VisualEditor11",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeDocument",
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
    "arn:aws:ssm:*:*:document/AWSMigration-*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "VisualEditor12",
  "Effect" : "Allow",
  "Action" : [
    "drs:DisconnectSourceServer"
  ],
  "Resource" : "arn:aws:drs:*:*:source-server/*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    },
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
    }
  }
}

```



```

    }
  },
  {
    "Sid" : "VisualEditor13",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameter",
      "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
  },
  {
    "Sid" : "VisualEditor14",
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "VisualEditor15",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
  },
  {
    "Sid" : "VisualEditor16",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetDocument"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
      "arn:aws:ssm:*:*:document/AWSMigration-*"
    ]
  },
  {
    "Sid" : "VisualEditor17",
    "Effect" : "Allow",
    "Action" : [

```

```

    "ssm:GetParameters"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "ssm.amazonaws.com"
    }
  }
},
{
  "Sid" : "VisualEditor18",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution"
  ],
  "Resource" : "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "mgn.amazonaws.com"
    }
  }
},
{
  "Sid" : "VisualEditor19",
  "Effect" : "Allow",
  "Action" : "ssm:ListCommands",
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "ssm.amazonaws.com"
    }
  }
},
{
  "Sid" : "VisualEditor20",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeParameters"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [

```

```
        "mgn.amazonaws.com"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationMGHAccess

Descrizione: questa politica consente all' AWS Application Migration Service (MGN) di inviare metadati sullo stato di avanzamento dei server in fase di migrazione tramite MGN a Migration AWS Hub (MGH). MGN crea automaticamente un ruolo IAM con questa policy allegata e assume questo ruolo. Non è consigliabile collegare questa policy ai propri utenti o ruoli IAM.

AWSApplicationMigrationMGHAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationMGHAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 aprile 2021, 07:10 UTC
- Ora modificata: 07 aprile 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationReadOnlyAccess

Descrizione: questa policy fornisce le autorizzazioni per tutte le API pubbliche di sola lettura di Application Migration Service (MGN), nonché per alcune API di sola lettura di altri AWS servizi necessarie per utilizzare appieno la console MGN in sola lettura. Allega questa policy ai tuoi utenti o ruoli IAM.

AWSApplicationMigrationReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 aprile 2021, 07:15 UTC
- Ora modificata: 20 marzo 2023, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationReplicationServerPolicy

Descrizione: questa policy consente ai server di replica di Application Migration Service (MGN), che sono istanze EC2 lanciate da Application Migration Service, di comunicare con il servizio MGN e di creare istantanee EBS all'interno dell'utente. Account AWS Un ruolo IAM con questa policy è associato (come profilo di istanza EC2) da Application Migration Service ai server di replica MGN, che vengono avviati e terminati automaticamente da MGN, in base alle esigenze. I server di replica MGN vengono utilizzati per facilitare la replica dei dati dai server esterni a AWS, come parte del processo di migrazione gestito tramite MGN. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

AWSApplicationMigrationReplicationServerPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationReplicationServerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 aprile 2021, 07:21 UTC
- Ora modificata: 07 aprile 2021, 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationServiceEc2InstancePolicy

Descrizione: questa policy consente l'installazione e l'utilizzo del AWS Replication Agent, utilizzato da AWS Application Migration Service (AWS MGN) per migrare i server di origine eseguiti su EC2 (Cross-region o Cross-AZ). Un ruolo IAM con questa policy deve essere allegato (come profilo di istanza EC2) alle istanze EC2.

AWSApplicationMigrationServiceEc2InstancePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti `AWSElasticLoadBalancingV2InstanceProfilePolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 agosto 2023, 13:19 UTC
- Ora modificata: 03 gennaio 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticLoadBalancingV2InstanceProfilePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationServiceRolePolicy

Descrizione: consente a AWS Application Migration Service di creare e gestire AWS risorse per conto dell'utente.

AWSApplicationMigrationServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 7 aprile 2021, 06:43 UTC
- Ora modificata: 20 giugno 2023, 09:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationSSMAccess

Descrizione: questa policy fornisce l'accesso alle operazioni di Amazon SSM necessarie per utilizzare Application Migration Service (MGN) per eseguire documenti SSM con comandi post-migrazione personalizzati. Allega questa policy ai tuoi utenti o ruoli IAM.

AWSApplicationMigrationSSMAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationSSMAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 09:29 UTC
- Ora modificata: 20 marzo 2023, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSApplicationMigrationVCenterClientPolicy

Descrizione: questa policy consente l'installazione e l'utilizzo del AWS vCenter Client, utilizzato con AWS Application Migration Service (MGN) per migrare server esterni verso AWS. AWS Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante l'installazione del vCenter Client.

AWS

AWSApplicationMigrationVCenterClientPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSApplicationMigrationVCenterClientPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 08 novembre 2021, 12:53 UTC
- Ora modificata: 08 novembre 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppMeshEnvoyAccess

Descrizione: policy di App Mesh Envoy per l'accesso alla configurazione del nodo virtuale.

AWSAppMeshEnvoyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppMeshEnvoyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 luglio 2019, 21:29 UTC
- Ora modificata: 03 luglio 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppMeshFullAccess

Descrizione: fornisce l'accesso completo alle API AWS App Mesh e alla console di gestione.

AWSAppMeshFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppMeshFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2019, 17:50 UTC
- Ora modificata: 07 gennaio 2021, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppMeshPreviewEnvoyAccess

Descrizione: policy di App Mesh Preview Envoy per l'accesso alla configurazione del nodo virtuale.

AWSAppMeshPreviewEnvoyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppMeshPreviewEnvoyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 agosto 2019, 23:32 UTC
- Ora modificata: 5 agosto 2019, 23:32 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppMeshPreviewServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da AWS App Mesh

AWSAppMeshPreviewServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 giugno 2019, 19:07 UTC
- Ora modificata: 21 agosto 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
    }
  ]
}
```

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppMeshReadOnly

Descrizione: fornisce accesso in sola lettura alle API AWS App Mesh e alla console di gestione.

AWSAppMeshReadOnly è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSAppMeshReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2019, 17:51 UTC
- Ora modificata: 07 gennaio 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppMeshServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da AWS AppMesh

AWSAppMeshServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 3 giugno 2019, 18:30 UTC
- Ora modificata: 10 ottobre 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
"Effect" : "Allow",
"Action" : [
  "servicediscovery:DiscoverInstances",
  "servicediscovery:DiscoverInstancesRevision"
],
"Resource" : "*"
},
{
  "Sid" : "ACMCertificateVerification",
  "Effect" : "Allow",
  "Action" : [
    "acm:DescribeCertificate"
  ],
  "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppRunnerFullAccess

Descrizione: concede le autorizzazioni a tutte le azioni di App Runner.

AWSAppRunnerFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSAppRunnerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 gennaio 2022, 04:02 UTC
- Ora modificata: 11 gennaio 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppRunnerReadOnlyAccess

Descrizione: concede le autorizzazioni per elencare e visualizzare i dettagli sulle risorse di App Runner.

AWSAppRunnerReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSAppRunnerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 febbraio 2022, 21:24 UTC
- Ora modificata: 24 febbraio 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "apprunner:List*",
      "apprunner:Describe*"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppRunnerServicePolicyForECRAccess

Descrizione: policy del servizio AWS App Runner che concede autorizzazioni di lettura alle risorse Amazon ECR nell'account del cliente. Usala in un ruolo che viene passato ad App Runner durante la creazione o l'aggiornamento di un servizio App Runner.

AWSAppRunnerServicePolicyForECRAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppRunnerServicePolicyForECRAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 maggio 2021, 19:17 UTC
- Ora modificata: 14 maggio 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppSyncAdministrator

Descrizione: fornisce l'accesso amministrativo al AppSync servizio, anche se non sufficiente per l'accesso tramite la console.

AWSAppSyncAdministrator è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppSyncAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 marzo 2018, 21:20 UTC
- Ora modificata: 04 novembre 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppSyncInvokeFullAccess

Descrizione: fornisce l'accesso completo al AppSync servizio tramite invocazione, sia tramite la console che in modo indipendente

AWSAppSyncInvokeFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppSyncInvokeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 marzo 2018, 21:21 UTC
- Ora modificata: 20 marzo 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppSyncPushToCloudWatchLogs

Descrizione: consente di AppSync inviare i log all' CloudWatch account dell'utente.

AWSAppSyncPushToCloudWatchLogs è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppSyncPushToCloudWatchLogs ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 09 aprile 2018, 19:38 UTC
- Ora modificata: 09 aprile 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppSyncSchemaAuthor

Descrizione: fornisce l'accesso per creare, aggiornare e interrogare lo schema.

AWSAppSyncSchemaAuthor è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSAppSyncSchemaAuthor ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 marzo 2018, 21:21 UTC
- Ora modificata: 01 febbraio 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAppSyncServiceRolePolicy

Descrizione: consente l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da AppSync

AWSAppSyncServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 gennaio 2020, 19:56 UTC
- Ora modificata: 21 gennaio 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSArtifactAccountSync

Descrizione: consente AWS l'accesso in sola lettura di Artifact alle operazioni in Organizations. AWS

AWSArtifactAccountSync è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSArtifactAccountSync ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 aprile 2018, 23:04 UTC

- Ora modificata: 10 aprile 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSArtifactReportsReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ai report del servizio Artifact AWS .

AWSArtifactReportsReadOnlyAccess [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSArtifactReportsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 gennaio 2024, 22:42 UTC
- Ora modificata: 02 gennaio 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSArtifactServiceRolePolicy

Descrizione: consente a AWS Artifact di raccogliere informazioni su un'organizzazione tramite AWS il servizio Organizations.

AWSArtifactServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 agosto 2023, 20:27 UTC
- Ora modificata: 21 agosto 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAuditManagerAdministratorAccess

Descrizione: Fornisce l'accesso amministrativo per abilitare o disabilitare AWS Audit Manager, aggiornare le impostazioni e gestire valutazioni, controlli e framework

AWSAuditManagerAdministratorAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSAuditManagerAdministratorAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2020, 20:02 UTC
- Ora modificata: 15 maggio 2024, 23:46 UTC

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

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
```

```

        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLikeIfExists" : {
            "organizations:ServicePrincipal" : [
                "auditmanager.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "IAMAccess",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
    ],
    "Resource" : "*"
},
{
    "Sid" : "IAMAccessCreateSLR",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "auditmanager.amazonaws.com"
        }
    }
},
{
    "Sid" : "IAMAccessManageSLR",
    "Effect" : "Allow",
    "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:UpdateRoleDescription",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
}

```

```
{,
{
  "Sid" : "S3Access",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsCreateGrantAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : "auditmanager.*.amazonaws.com"
    }
  }
},
{
  "Sid" : "SNSAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
```

```

    "Sid" : "CreateEventsAccess",
    "Effect" : "Allow",
    "Action" : [
        "events:PutRule"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
            "events:source" : [
                "aws.securityhub"
            ]
        }
    }
},
{
    "Sid" : "EventsAccess",
    "Effect" : "Allow",
    "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
},
{
    "Sid" : "TagAccess",
    "Effect" : "Allow",
    "Action" : [
        "tag:GetResources"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ControlCatalogAccess",
    "Effect" : "Allow",
    "Action" : [
        "controlcatalog:ListCommonControls",

```

```
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAuditManagerServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da AWS Audit Manager

AWSAuditManagerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 08 dicembre 2020, 15:12 UTC
- Ora modificata: 10 giugno 2024, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
```

```
"dynamodb:DescribeTableReplicaAutoScaling",
"dynamodb:DescribeTable",
"dynamodb:ListBackups",
"dynamodb:ListGlobalTables",
"dynamodb:ListTables",
"ec2:DescribeInstanceCreditSpecifications",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:GetLaunchTemplateData",
"ec2:DescribeAddresses",
"ec2:DescribeCustomerGateways",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeFlowLogs",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:DescribeLocalGateways",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeTransitGateways",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetEbsDefaultKmsKeyId",
"ec2:GetEbsEncryptionByDefault",
"ecs:DescribeClusters",
"eks:DescribeAddonVersions",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeServiceUpdates",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeSslPolicies",
"elasticloadbalancing:DescribeTargetGroups",
"elasticmapreduce:ListClusters",
```



```
"elasticmapreduce:ListSecurityConfigurations",
"events:DescribeRule",
"events:ListConnections",
"events:ListEventBuses",
"events:ListEventSources",
"events:ListRules",
"firehose:ListDeliveryStreams",
"fsx:DescribeFileSystems",
"guardduty:ListDetectors",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccessKeyLastUsed",
"iam:GetCredentialReport",
"iam:GetGroupPolicy",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:GetUserPolicy",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:ListAttachedGroupPolicies",
"iam:ListAttachedUserPolicies",
"iam:ListEntitiesForPolicy",
"iam:ListGroupsForUser",
"iam:ListGroupPolicies",
"iam:ListGroups",
"iam:ListOpenIdConnectProviders",
"iam:ListPolicies",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListSamlProviders",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"iam:ListPolicyVersions",
"iam:ListAccessKeys",
"iam:ListAttachedRolePolicies",
"iam:ListMfaDeviceTags",
"iam:ListMfaDevices",
"kafka:ListClusters",
"kafka:ListKafkaVersions",
"kinesis:ListStreams",
"kms:DescribeKey",
```

```
"kms:GetKeyPolicy",
"kms:GetKeyRotationStatus",
"kms:ListGrants",
"kms:ListKeyPolicies",
"kms:ListKeys",
"lambda:ListFunctions",
"license-manager:ListAssociationsForLicenseConfiguration",
"license-manager:ListLicenseConfigurations",
"license-manager:ListUsageForLicenseConfiguration",
"logs:DescribeDestinations",
"logs:DescribeExportTasks",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"logs:DescribeResourcePolicies",
"logs:FilterLogEvents",
"logs:GetDataProtectionPolicy",
"es:DescribeDomains",
"es:DescribeDomain",
"es:DescribeDomainConfig",
"es:ListDomainNames",
"organizations:DescribeOrganization",
"organizations:DescribePolicy",
"rds:DescribeCertificates",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBInstances",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBInstanceAutomatedBackups",
"redshift:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeLoggingStatus",
"route53:GetQueryLoggingConfig",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelCard",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeModel",
```

```

"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeUserProfile",
"sagemaker:ListAlgorithms",
"sagemaker:ListDomains",
"sagemaker:ListEndpoints",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListLabelingJobs",
"sagemaker:ListModels",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelCards",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListMonitoringAlerts",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListTrainingJobs",
"sagemaker:ListUserProfiles",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketVersioning",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3:ListAllMyBuckets",
"secretsmanager:DescribeSecret",
"secretsmanager:ListSecrets",
"securityhub:DescribeStandards",
"sns:ListTagsForResource",
"sns:ListTopics",
"sqs:ListQueues",
"waf-regional:GetRule",
"waf-regional:GetWebAcl",
"waf:GetRule",
"waf:GetRuleGroup",
"waf:ListActivatedRulesInRuleGroup",
"waf:ListWebAcls",
"wafv2:ListWebAcls",
"waf-regional:GetLoggingConfiguration",
"waf-regional:ListRuleGroups",
"waf-regional:ListSubscribedRuleGroups",
"waf-regional:ListWebACLs",
"waf-regional:ListRules",
"waf:ListRuleGroups",
"waf:ListRules"
],
"Resource" : "*",

```

```
    "Sid" : "APIsAccess"
  },
  {
    "Sid" : "S3Access",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketAcl",
      "s3:GetBucketLogging",
      "s3:GetBucketOwnershipControls",
      "s3:GetBucketPolicy",
      "s3:GetBucketTagging"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : [
          "${aws:PrincipalAccount}"
        ]
      }
    }
  },
  {
    "Sid" : "APIGatewayAccess",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET"
    ],
    "Resource" : [
      "arn:aws:apigateway:*::/restapis",
      "arn:aws:apigateway:*::/restapis/*/stages/*",
      "arn:aws:apigateway:*::/restapis/*/stages"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : [
          "${aws:PrincipalAccount}"
        ]
      }
    }
  },
  {
    "Sid" : "CreateEventsAccess",
    "Effect" : "Allow",
    "Action" : [
```

```
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
  "Condition" : {
    "StringEquals" : {
      "events:detail-type" : "Security Hub Findings - Imported"
    },
    "Null" : {
      "events:source" : "false"
    },
    "ForAllValues:StringEquals" : {
      "events:source" : [
        "aws.securityhub"
      ]
    }
  }
},
{
  "Sid" : "EventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

Descrizione: politica che concede le autorizzazioni ad Auto AWS Scaling per prevedere periodicamente la capacità e generare azioni di scaling pianificate per i gruppi di Auto Scaling in un piano di scalabilità

AWSAutoScalingPlansEC2AutoScalingPolicy è una [AWS politica](#) gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 agosto 2018, 22:46 UTC
- Ora modificata: 23 agosto 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupAuditAccess

Descrizione: questa politica concede agli utenti le autorizzazioni per creare controlli e framework che definiscono le loro aspettative per le risorse e le attività di AWS Backup e per controllare le risorse e le attività di AWS Backup rispetto ai controlli e ai framework definiti. Questa politica concede le autorizzazioni a AWS Config e servizi simili per descrivere le aspettative degli utenti, eseguire gli audit. Questa politica concede anche le autorizzazioni per fornire report di controllo a S3 e servizi simili e consente agli utenti di trovare e aprire i propri report di controllo.

AWSBackupAuditAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSBackupAuditAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 agosto 2021, 01:02 UTC
- Ora modificata: 10 aprile 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:::*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupDataTransferAccess

Descrizione: questa politica consente all'agente AWS Backint di completare il trasferimento dei dati di backup con il piano AWS Backup Storage. Associa questa policy ai ruoli assunti dalle istanze EC2 che eseguono SAP HANA con l'agente Backint.

AWSBackupDataTransferAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSBackupDataTransferAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 10 novembre 2022, 22:48 UTC
- Ora modificata: 10 novembre 2022, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupFullAccess

Descrizione: questa politica è destinata agli amministratori di backup e concede l'accesso completo alle operazioni di AWS backup, inclusa la creazione o la modifica dei piani di backup, l'assegnazione di AWS risorse ai piani di backup, l'eliminazione dei backup e il ripristino dei backup.

AWSBackupFullAccess è una [politica](#) gestita AWS.

Utilizzo di questa politica

Puoi collegarti AWSBackupFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 novembre 2019, 22:21 UTC
- Ora modificata: 27 novembre 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Versione della politica

Versione della politica: v17 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "ram:GetResourceShareAssociations"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Descrizione: fornisce AWS BackupGateway l'autorizzazione a sincronizzare i metadati delle macchine virtuali per tuo conto

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio

- Ora di creazione: 15 dicembre 2022, 19:43 UTC
- Ora modificata: 15 dicembre 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupOperatorAccess

Descrizione: questa politica concede agli utenti le autorizzazioni per assegnare AWS risorse ai piani di backup, creare backup su richiesta e ripristinare i backup. Questa politica non consente all'utente di creare o modificare piani di backup o di eliminare i backup pianificati dopo la creazione.

AWSBackupOperatorAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBackupOperatorAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 novembre 2019, 22:23 UTC
- Ora modificata: 06 settembre 2023, 20:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupOrganizationAdminAccess

Descrizione: questa policy è destinata agli amministratori di backup che utilizzano la gestione dei backup tra account per gestire i backup per l'organizzazione.

AWSBackupOrganizationAdminAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti `AWSSBackupOrganizationAdminAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 16:23 UTC
- Ora modificata: 18 novembre 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSBackupOrganizationAdminAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupRestoreAccessForSAPHANA

Descrizione: Fornisce l'autorizzazione di AWS backup per ripristinare un backup di SAP HANA su Amazon EC2

AWSBackupRestoreAccessForSAPHANA [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSBackupRestoreAccessForSAPHANA ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2022, 22:43 UTC
- Ora modificata: 10 novembre 2022, 22:43 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*"  
  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupServiceLinkedRolePolicyForBackup

Descrizione: Fornisce l'autorizzazione AWS di Backup per creare backup per conto dell'utente su tutti AWS i servizi

AWSBackupServiceLinkedRolePolicyForBackup è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 2 giugno 2020, 23:08 UTC
- Ora modificata: 17 maggio 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Versione della politica

Versione della politica: v16 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
},
{
    "Sid" : "RecoveryPointTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
        "backup:TagResource"
    ],
    "Resource" : "arn:aws:backup:*:*:recovery-point:*",
    "Condition" : {
        "StringEquals" : {
            "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
    }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

Descrizione: Fornisce l'autorizzazione di AWS Backup per creare backup per conto dell'utente su più AWS servizi

AWSBackupServiceLinkedRolePolicyForBackupTest è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 maggio 2020, 17:37 UTC
- Ora modificata: 12 maggio 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupServiceRolePolicyForBackup

Descrizione: Fornisce l'autorizzazione AWS di Backup per creare backup per conto dell'utente su tutti AWS i servizi

AWSBackupServiceRolePolicyForBackup è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBackupServiceRolePolicyForBackup ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 gennaio 2019, 21:01 UTC
- Ora modificata: 17 maggio 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Versione della politica

Versione della politica: v19 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*"
},
{

```



```
"Sid" : "RecoveryPointTaggingPermissions",
"Effect" : "Allow",
"Action" : [
  "backup:TagResource"
],
"Resource" : "arn:aws:backup:*:*:recovery-point:*",
"Condition" : {
  "StringEquals" : {
    "aws:PrincipalAccount" : "${aws:ResourceAccount}"
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupServiceRolePolicyForRestores

Descrizione: Fornisce l'autorizzazione AWS di Backup per eseguire ripristini per conto dell'utente su tutti AWS i servizi. Questa politica include le autorizzazioni per creare ed eliminare AWS risorse, come volumi EBS, istanze RDS e file system EFS, che fanno parte del processo di ripristino.

AWSBackupServiceRolePolicyForRestores [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSBackupServiceRolePolicyForRestores ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 gennaio 2019, 00:23 UTC
- Ora modificata: 15 dicembre 2023, 22:05 UTC

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

Versione della politica

Versione della politica: v20 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "KMSTDescribePermissions",
  "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" : "KMSTCreateGrantPermissions",
  "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" : [
        "*"
    ]
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupServiceRolePolicyForS3Backup

Descrizione: policy contenente le autorizzazioni necessarie per il AWS Backup per il backup dei dati in qualsiasi bucket S3. Ciò include l'accesso in lettura a tutti gli oggetti S3 e qualsiasi accesso di decrittografia per tutte le chiavi KMS.

AWSBackupServiceRolePolicyForS3Backup è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSBackupServiceRolePolicyForS3Backup ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 febbraio 2022, 17:40 UTC
- Ora modificata: 17 maggio 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchGetMetricDataPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgePermissionsForAwsBackupManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeListRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
    "StringLike" : {
      "kms:ViaService" : "s3.*.amazonaws.com"
    }
  },
  {
    "Sid" : "S3BucketPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketTagging",
      "s3:GetInventoryConfiguration",
      "s3:ListBucketVersions",
      "s3:ListBucket",
      "s3:GetBucketVersioning",
      "s3:GetBucketLocation",
      "s3:GetBucketAcl",
      "s3:PutInventoryConfiguration",
      "s3:GetBucketNotification",
      "s3:PutBucketNotification"
    ],
    "Resource" : "arn:aws:s3:::*"
  },
  {
    "Sid" : "S3ObjectPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObjectAcl",
      "s3:GetObject",
      "s3:GetObjectVersionTagging",
      "s3:GetObjectVersionAcl",
      "s3:GetObjectTagging",
      "s3:GetObjectVersion"
    ],
    "Resource" : "arn:aws:s3:::*/*"
  },
  {
    "Sid" : "S3ListBucketPermissions",
    "Effect" : "Allow",
    "Action" : "s3:ListAllMyBuckets",
    "Resource" : "*"
  },
  {
    "Sid" : "RecoveryPointTaggingPermissions",
    "Effect" : "Allow",
```

```
"Action" : [
  "backup:TagResource"
],
"Resource" : "arn:aws:backup:*:*:recovery-point:*",
"Condition" : {
  "StringEquals" : {
    "aws:PrincipalAccount" : "${aws:ResourceAccount}"
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBackupServiceRolePolicyForS3Restore

Descrizione: policy contenente le autorizzazioni necessarie per consentire a AWS Backup di ripristinare un backup S3 in un bucket. Ciò include le autorizzazioni di lettura/scrittura per tutti i bucket S3 e le autorizzazioni per e per tutte le chiavi KMS. GenerateDataKey DescribeKey

AWSBackupServiceRolePolicyForS3Restore è [AWS una politica gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBackupServiceRolePolicyForS3Restore ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 febbraio 2022, 17:39 UTC
- Ora modificata: 07 febbraio 2023, 00:06 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBatchFullAccess

Descrizione: Fornisce l'accesso completo alle risorse AWS Batch.

AWSBatchFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBatchFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 dicembre 2016, 19:35 UTC
- Ora modificata: 24 ottobre 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBatchServiceEventTargetRole

Descrizione: politica per abilitare CloudWatch Event Target per l'invio di AWS Batch Job

AWSBatchServiceEventTargetRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBatchServiceEventTargetRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 febbraio 2018, 22:31 UTC
- Ora modificata: 28 febbraio 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBatchServiceRole

Descrizione: ruolo del servizio Policy for AWS Batch che consente l'accesso a servizi correlati tra cui EC2, Autoscaling, il servizio EC2 Container e Cloudwatch Logs.

AWSBatchServiceRole è una [AWS policy](#) gestita.

Utilizzo di questa politica

Puoi collegarti AWSBatchServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 dicembre 2016, 19:36 UTC
- Ora modificata: 05 dicembre 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBCMDDataExportsServiceRolePolicy

Descrizione: un ruolo collegato al servizio per fornire ai dati di Billing and Cost Management Exports l'accesso AWS ai dati del servizio per esportare i dati in una posizione di destinazione, come Amazon S3, per conto di un cliente.

AWSBCMDDataExportsServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 giugno 2024, 17:40 UTC
- Ora modificata: 10 giugno 2024, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDDataExportsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBillingConductorFullAccess

Descrizione: utilizza la policy AWSBillingConductorFullAccess gestita per consentire l'accesso completo alla console AWS Billing Conductor (ABC) e alle API. Questa politica consente agli utenti di elencare, creare ed eliminare risorse ABC.

AWSBillingConductorFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBillingConductorFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 aprile 2022, 18:02 UTC
- Ora modificata: 13 aprile 2022, 18:02 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBillingConductorReadOnlyAccess

Descrizione: utilizza la policy `AWSBillingConductorReadOnlyAccess` gestita per consentire l'accesso in sola lettura alla console AWS Billing Conductor (ABC) e alle API. Questa politica concede

l'autorizzazione a visualizzare ed elencare tutte le risorse ABC. Non include la possibilità di creare o eliminare risorse.

AWSBillingConductorReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBillingConductorReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 aprile 2022, 18:02 UTC
- Ora modificata: 13 aprile 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBillingReadOnlyAccess

Descrizione: consente agli utenti di visualizzare le fatture sulla Billing Console.

AWSBillingReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBillingReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 agosto 2020, 20:08 UTC
- Ora modificata: 23 maggio 2024, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Sid" : "VisualEditor0",
"Effect" : "Allow",
"Action" : [
  "account:GetAccountInformation",
  "aws-portal:ViewBilling",
  "billing:GetBillingData",
  "billing:GetBillingDetails",
  "billing:GetBillingNotifications",
  "billing:GetBillingPreferences",
  "billing:GetCredits",
  "billing:GetContractInformation",
  "billing:GetIAMAccessPreference",
  "billing:GetSellerOfRecord",
  "billing:ListBillingViews",
  "budgets:ViewBudget",
  "budgets:DescribeBudgetActionsForBudget",
  "budgets:DescribeBudgetAction",
  "budgets:DescribeBudgetActionsForAccount",
  "budgets:DescribeBudgetActionHistories",
  "ce:DescribeCostCategoryDefinition",
  "ce:GetCostAndUsage",
  "ce:ListCostCategoryDefinitions",
  "ce:ListTagsForResource",
  "ce:ListCostAllocationTags",
  "ce:ListCostAllocationTagBackfillHistory",
  "ce:GetTags",
  "ce:GetDimensionValues",
  "consolidatedbilling:ListLinkedAccounts",
  "consolidatedbilling:GetAccountBillingRole",
  "cur:GetClassicReport",
  "cur:GetClassicReportPreferences",
  "cur:GetUsageReport",
  "cur:DescribeReportDefinitions",
  "freetier:GetFreeTierAlertPreference",
  "freetier:GetFreeTierUsage",
  "invoicing:GetInvoiceEmailDeliveryPreferences",
  "invoicing:GetInvoicePDF",
  "invoicing:ListInvoiceSummaries",
  "payments:GetPaymentInstrument",
  "payments:GetPaymentStatus",
  "payments:ListPaymentPreferences",
  "payments:ListTagsForResource",
  "payments:ListPaymentInstruments",
  "purchase-orders:GetPurchaseOrder",
```

```
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Descrizione: questa politica fornisce le autorizzazioni per controllare AWS le risorse. Ad esempio, per avviare e arrestare le istanze EC2 o RDS eseguendo script AWS Systems Manager (SSM).

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 25 maggio 2022, 19:03 UTC

- Ora modificata: 25 maggio 2022, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBudgetsActionsWithAWSResourceControlAccess

Descrizione: fornisce l'accesso completo a AWS Budgets Actions, incluso l'utilizzo di Budgets Actions per controllare lo stato delle risorse in esecuzione AWS tramite AWS Management Console

AWSBudgetsActionsWithAWSResourceControlAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBudgetsActionsWithAWSResourceControlAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 ottobre 2020, 17:19 UTC
- Ora modificata: 15 ottobre 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBudgetsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Budgets Console tramite. AWS Management Console

AWSBudgetsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBudgetsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 ottobre 2020, 17:18 UTC

- Ora modificata: 15 ottobre 2020, 17:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBugBustFullAccess

Descrizione: questa policy IAM garantisce agli utenti l'accesso completo alla console AWS BugBust

AWSBugBustFullAccess è una [policy AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBugBustFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2021, 07:03 UTC
- Ora modificata: 22 luglio 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBugBustPlayerAccess

Descrizione: questa policy IAM consente agli utenti di accedere alla partecipazione AWS BugBust agli eventi

AWSBugBustPlayerAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSBugBustPlayerAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2021, 07:15 UTC
- Ora modificata: 24 giugno 2021, 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSBugBustServiceRolePolicy

Descrizione: concede le autorizzazioni per accedere AWS BugBust alle risorse per tuo conto

AWSBugBustServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 giugno 2021, 06:59 UTC
- Ora modificata: 24 giugno 2021, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCertificateManagerFullAccess

Descrizione: Fornisce l'accesso completo a AWS Certificate Manager (ACM)

AWSCertificateManagerFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCertificateManagerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 gennaio 2016, 17:02 UTC
- Ora modificata: 17 agosto 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCertificateManagerPrivateCAAuditor

Descrizione: Fornisce l'accesso dei revisori all'autorità di certificazione privata di AWS Certificate Manager

AWSCertificateManagerPrivateCAAuditor è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSCertificateManagerPrivateCAAuditor` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 ottobre 2018, 16:51 UTC
- Ora modificata: 17 agosto 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCertificateManagerPrivateCAFullAccess

Descrizione: Fornisce l'accesso completo all'autorità di AWS certificazione privata di Certificate Manager

AWSCertificateManagerPrivateCAFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCertificateManagerPrivateCAFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 ottobre 2018, 16:54 UTC
- Ora modificata: 23 ottobre 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCertificateManagerPrivateCAPrivilegedUser

Descrizione: fornisce agli utenti dei certificati l'accesso privilegiato all'autorità di certificazione privata di AWS Certificate Manager

AWSCertificateManagerPrivateCAPrivilegedUser è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCertificateManagerPrivateCAPrivilegedUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 giugno 2019, 17:43 UTC
- Ora modificata: 20 giugno 2019, 17:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCertificateManagerPrivateCAReadOnly

Descrizione: fornisce l'accesso in sola lettura all'autorità di AWS certificazione privata di Certificate Manager

AWSCertificateManagerPrivateCAReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSCertificateManagerPrivateCAReadOnly` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 ottobre 2018, 16:57 UTC
- Ora modificata: 17 agosto 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCertificateManagerPrivateCAUser

Descrizione: Fornisce agli utenti del certificato l'accesso all'autorità di AWS certificazione privata di Certificate Manager

AWSCertificateManagerPrivateCAUser è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCertificateManagerPrivateCAUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 ottobre 2018, 16:53 UTC
- Ora modificata: 20 giugno 2019, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCertificateManagerReadOnly

Descrizione: fornisce l'accesso in sola lettura a AWS Certificate Manager (ACM).

AWSCertificateManagerReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCertificateManagerReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 gennaio 2016, 17:07 UTC
- Ora modificata: 15 marzo 2021, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSChatbotServiceLinkedRolePolicy

Descrizione: il ruolo collegato al servizio utilizzato dal AWS Chatbot.

AWSChatbotServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 novembre 2019, 16:39 UTC

- Ora modificata: 18 novembre 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCleanRoomsFullAccess

Descrizione: consente l'accesso completo alle risorse di AWS Clean Rooms e l'accesso alle risorse correlate Servizi AWS.

AWSCleanRoomsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCleanRoomsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2023, 16:10 UTC
- Ora modificata: 21 marzo 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

```

    "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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCleanRoomsFullAccessNoQuerying

Descrizione: consente l'accesso completo alle risorse di AWS Clean Rooms ad eccezione delle interrogazioni in collaborazione e dell'accesso alle risorse correlate Servizi AWS.

AWSCleanRoomsFullAccessNoQuerying è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCleanRoomsFullAccessNoQuerying ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2023, 16:12 UTC
- Ora modificata: 14 maggio 2024, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms>DeleteAnalysisTemplate",
        "cleanrooms>DeleteCollaboration",
        "cleanrooms>DeleteConfiguredTable",
        "cleanrooms>DeleteConfiguredTableAnalysisRule",
        "cleanrooms>DeleteConfiguredTableAssociation",
        "cleanrooms>DeleteMember",
        "cleanrooms>DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
```

```

        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CleanRoomsNoQuerying",
    "Effect" : "Deny",
    "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
    ],
    "Resource" : "*"
},
{
    "Sid" : "PassServiceRole",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
    }
},
{
    "Sid" : "ListRolesToPickServiceRole",
    "Effect" : "Allow",
    "Action" : [
        "iam:ListRoles"
    ]
}

```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole",
      "iam:ListRolePolicies",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
  },
  {
    "Sid" : "ListPoliciesToInspectServiceRolePolicy",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListPolicies"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GetPolicyToInspectServiceRolePolicy",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetPolicy",
      "iam:GetPolicyVersion"
    ],
    "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
  },
  {
    "Sid" : "ConsoleDisplayTables",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:GetSchema",
      "glue:GetSchemaVersion",
      "glue:BatchGetPartition"
    ]
  },
],
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "EstablishLogDeliveries",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs:GetLogDelivery",
      "logs:UpdateLogDelivery",
      "logs>DeleteLogDelivery",
      "logs:ListLogDeliveries"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SetupLogGroupsDescribe",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SetupLogGroupsCreate",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  }
}
```



```
{,
{
  "Sid" : "SetupLogGroupsResourcePolicy",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeResourcePolicies",
    "logs:PutResourcePolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
  }
},
{
  "Sid" : "ConsoleLogSummaryQueryLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:StartQuery"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
},
{
  "Sid" : "ConsoleLogSummaryObtainLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:GetQueryResults"
  ],
  "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCleanRoomsMLFullAccess

Descrizione: consente l'accesso completo alle risorse AWS Clean Rooms ML e l'accesso alle relative Servizi AWS.

AWSCleanRoomsMLFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCleanRoomsMLFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2023, 21:02 UTC
- Ora modificata: 29 novembre 2023, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCleanRoomsMLReadOnlyAccess

Descrizione: consente l'accesso in sola lettura alle risorse AWS Clean Rooms ML e l'accesso in sola lettura alle risorse Clean Rooms correlate AWS

AWSCleanRoomsMLReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSCleanRoomsMLReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2023, 20:55 UTC
- Ora modificata: 29 novembre 2023, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCleanRoomsReadOnlyAccess

Descrizione: consente l'accesso in sola lettura alle risorse AWS Clean Rooms e l'accesso in sola lettura alle risorse AWS Glue e Amazon Logs correlate. CloudWatch

AWSCleanRoomsReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSCleanRoomsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2023, 16:10 UTC
- Ora modificata: 12 gennaio 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloud9Administrator

Descrizione: fornisce l'accesso come amministratore a AWS Cloud9.

AWSCloud9Administrator è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloud9Administrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:17 UTC
- Ora modificata: 11 ottobre 2023, 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloud9EnvironmentMember

Descrizione: offre la possibilità di essere invitato negli ambienti di sviluppo AWS condivisi Cloud9.

AWSCloud9EnvironmentMember è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloud9EnvironmentMember ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:18 UTC
- Ora modificata: 11 ottobre 2023, 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloud9ServiceRolePolicy

Descrizione: policy Service Linked Role per AWS Cloud9

AWSCloud9ServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi

- Ora di creazione: 30 novembre 2017, 13:44 UTC
- Ora modificata: 17 gennaio 2022, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloud9SSMInstanceProfile

Descrizione: questa policy verrà utilizzata per assegnare un ruolo a Cloud9 di utilizzare SSM Session Manager per connettersi all'istanza InstanceProfile

AWSCloud9SSMInstanceProfile [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti `AWSCloud9SSMInstanceProfile` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 maggio 2020, 11:40 UTC
- Ora modificata: 14 maggio 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloud9User

Descrizione: Fornisce l'autorizzazione per creare AWS ambienti di sviluppo Cloud9 e gestire ambienti di proprietà.

AWSCloud9User è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloud9User ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:16 UTC
- Ora modificata: 11 ottobre 2023, 13:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudFormationFullAccess

Descrizione: Fornisce accesso completo a AWS CloudFormation.

AWSCloudFormationFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudFormationFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2019, 21:50 UTC
- Ora modificata: 26 luglio 2019, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudFormationReadOnlyAccess

Descrizione: Fornisce l'accesso AWS CloudFormation tramite AWS Management Console.

AWSCloudFormationReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudFormationReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 13 novembre 2019, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWS CloudFront Logger

Descrizione: concede a CloudFront Logger i permessi di scrittura per Logs. CloudWatch

AWSCloudFrontLogger [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 giugno 2018, 20:15 UTC
- Ora modificata: 22 novembre 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudHSMFullAccess

Descrizione: fornisce l'accesso completo a tutte le risorse CloudHSM.

AWSCloudHSMFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudHSMFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudHSMReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a tutte le risorse CloudHSM.

AWSCloudHSMReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudHSMReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudHSMRole

Descrizione: policy predefinita per il ruolo del servizio AWS CloudHSM.

AWSCloudHSMRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudHSMRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC

- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudMapDiscoverInstanceAccess

Descrizione: fornisce l'accesso all'API Cloud AWS Map Discovery.

AWSCloudMapDiscoverInstanceAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudMapDiscoverInstanceAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2018, 00:02 UTC
- Ora modificata: 20 settembre 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudMapFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni della Cloud AWS mappa.

AWSCloudMapFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudMapFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 23:57 UTC
- Ora modificata: 29 luglio 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudMapReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutte le azioni della Cloud AWS mappa.

AWSCloudMapReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudMapReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 23:45 UTC
- Ora modificata: 20 settembre 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudMapRegisterInstanceAccess

Descrizione: fornisce l'accesso a livello di registrante alle azioni della Cloud AWS mappa.

AWSCloudMapRegisterInstanceAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudMapRegisterInstanceAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2018, 00:04 UTC
- Ora modificata: 20 settembre 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudShellFullAccess

Descrizione: concede l'utilizzo AWS CloudShell con tutte le funzionalità

AWSCloudShellFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudShellFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 18:07 UTC
- Ora modificata: 15 dicembre 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudTrail_FullAccess

Descrizione: fornisce accesso completo a AWS CloudTrail.

AWSCloudTrail_FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSCloudTrail_FullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 ottobre 2020, 23:41 UTC
- Ora modificata: 22 febbraio 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudTrail_ReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a AWS CloudTrail.

AWSCloudTrail_ReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCloudTrail_ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 14 giugno 2022, 17:19 UTC
- Ora modificata: 14 giugno 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Descrizione: questo criterio viene utilizzato dal ruolo collegato al servizio denominato.

AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents CloudWatch utilizza questo ruolo collegato al servizio per eseguire azioni di AWS System Manager Incident Manager quando un CloudWatch allarme entra nello stato ALARM. Questa politica concede il permesso di avviare incidenti per conto dell'utente.

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 27 aprile 2021, 13:30 UTC
- Ora modificata: 27 aprile 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeArtifactAdminAccess

Descrizione: Fornisce l'accesso completo AWS CodeArtifact tramite AWS Management Console.

AWSCodeArtifactAdminAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeArtifactAdminAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 16 giugno 2020, 23:53 UTC
- Ora modificata: 16 giugno 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeArtifactReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura AWS CodeArtifact tramite AWS Management Console.

AWSCodeArtifactReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeArtifactReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 giugno 2020, 21:23 UTC
- Ora modificata: 25 giugno 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeBuildAdminAccess

Descrizione: Fornisce l'accesso completo AWS CodeBuild tramite AWS Management Console. Collega anche AmazonS3 ReadOnlyAccess per fornire l'accesso al download degli artefatti della build e collega IAM FullAccess per creare e gestire il ruolo di servizio per CodeBuild

AWSCodeBuildAdminAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSCodeBuildAdminAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 19:04 UTC
- Ora modificata: 02 maggio 2024, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
```

```

        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
},
{
    "Sid" : "CWLDeleteLogGroupAccess",
    "Action" : [
        "logs:DeleteLogGroup"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
},
{
    "Sid" : "SSMParameterWriteAccess",
    "Effect" : "Allow",
    "Action" : [
        "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
},
{
    "Sid" : "SSMStartSessionAccess",
    "Effect" : "Allow",
    "Action" : [

```

```

    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
},
{
  "Sid" : "CodeStarConnectionsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:CreateConnection",
    "codestar-connections>DeleteConnection",
    "codestar-connections:UpdateConnectionInstallation",
    "codestar-connections:TagResource",
    "codestar-connections:UntagResource",
    "codestar-connections:ListConnections",
    "codestar-connections:ListInstallationTargets",
    "codestar-connections:ListTagsForResource",
    "codestar-connections:GetConnection",
    "codestar-connections:GetIndividualAccessToken",
    "codestar-connections:GetInstallationUrl",
    "codestar-connections:PassConnection",
    "codestar-connections:StartOAuthHandshake",
    "codestar-connections:UseConnection"
  ],
  "Resource" : [
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
  ]
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeBuildDeveloperAccess

Descrizione: fornisce l'accesso AWS CodeBuild tramite AWS Management Console, ma non consente l'amministrazione CodeBuild del progetto. Inoltre, collega AmazonS3 ReadOnlyAccess per consentire l'accesso al download degli artefatti della build.

AWSCodeBuildDeveloperAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSCodeBuildDeveloperAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 19:02 UTC
- Ora modificata: 02 maggio 2024, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```

"Statement" : [
  {
    "Sid" : "AWSServicesAccess",
    "Action" : [
      "codebuild:StartBuild",
      "codebuild:StopBuild",
      "codebuild:StartBuildBatch",
      "codebuild:StopBuildBatch",
      "codebuild:RetryBuild",
      "codebuild:RetryBuildBatch",
      "codebuild:BatchGet*",
      "codebuild:GetResourcePolicy",
      "codebuild:DescribeTestCases",
      "codebuild:DescribeCodeCoverages",
      "codebuild:List*",
      "codecommit:GetBranch",
      "codecommit:GetCommit",
      "codecommit:GetRepository",
      "codecommit:ListBranches",
      "cloudwatch:GetMetricStatistics",
      "events:DescribeRule",
      "events:ListTargetsByRule",
      "events:ListRuleNamesByTarget",
      "logs:GetLogEvents",
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "SSMParameterWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
  },
  {
    "Sid" : "SSMStartSessionAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
  },

```

```

    "Resource" : "arn:aws:ecs:*:*:task/*/*"
  },
  {
    "Sid" : "CodeStarConnectionsUserAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:ListConnections",
      "codestar-connections:GetConnection"
    ],
    "Resource" : [
      "arn:aws:codestar-connections:*:*:connection/*",
      "arn:aws:codeconnections:*:*:connection/*"
    ]
  },
  {
    "Sid" : "CodeStarNotificationsReadWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:CreateNotificationRule",
      "codestar-notifications:DescribeNotificationRule",
      "codestar-notifications:UpdateNotificationRule",
      "codestar-notifications:Subscribe",
      "codestar-notifications:Unsubscribe"
    ],
    "Resource" : "*",
    "Condition" : {
      "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"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeBuildReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura AWS CodeBuild tramite AWS Management Console. Inoltre, collega AmazonS3 ReadOnlyAccess per consentire l'accesso al download degli artefatti della build.

AWSCodeBuildReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSCodeBuildReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 19:03 UTC
- Ora modificata: 02 maggio 2024, 01:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```

    "Sid" : "CodeStarConnectionsUserAccess",
    "Effect" : "Allow",
    "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
    ],
    "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
    ]
},
{
    "Sid" : "CodeStarNotificationsPowerUserAccess",
    "Effect" : "Allow",
    "Action" : [
        "codestar-notifications:DescribeNotificationRule"
    ],
    "Resource" : "*",
    "Condition" : {
        "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"
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeCommitFullAccess

Descrizione: Fornisce l'accesso completo AWS CodeCommit tramite AWS Management Console.

AWSCodeCommitFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeCommitFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:02 UTC
- Ora modificata: 17 luglio 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeCommitPowerUser

Descrizione: fornisce l'accesso completo ai AWS CodeCommit repository, ma non consente l'eliminazione degli archivi.

AWSCodeCommitPowerUser è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeCommitPowerUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:06 UTC
- Ora modificata: 17 luglio 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeCommitReadOnly

Descrizione: fornisce l'accesso in sola lettura AWS CodeCommit tramite AWS Management Console.

AWSCodeCommitReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeCommitReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:05 UTC
- Ora modificata: 18 agosto 2021, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployDeployerAccess

Descrizione: fornisce l'accesso per registrare e distribuire una revisione.

AWSCodeDeployDeployerAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeDeployDeployerAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 maggio 2015, 18:18 UTC
- Ora modificata: 2 aprile 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployFullAccess

Descrizione: fornisce l'accesso completo alle CodeDeploy risorse.

AWSCodeDeployFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSCodeDeployFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 maggio 2015, 18:13 UTC
- Ora modificata: 02 aprile 2020, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle CodeDeploy risorse.

AWSCodeDeployReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeDeployReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 maggio 2015, 18:21 UTC
- Ora modificata: 2 aprile 2020, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployRole

Descrizione: Fornisce l'accesso al CodeDeploy servizio per espandere i tag e interagire con Auto Scaling per tuo conto.

AWSCodeDeployRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeDeployRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 4 maggio 2015, 18:05 UTC
- Ora modificata: 16 agosto 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployRoleForCloudFormation

Descrizione: fornisce l'accesso al CodeDeploy servizio per richiamare la funzione Lambda per conto dell'utente per eseguire la distribuzione blu/verde. CloudFormation

AWSCodeDeployRoleForCloudFormation [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSCodeDeployRoleForCloudFormation ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 maggio 2020, 17:12 UTC
- Ora modificata: 19 maggio 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployRoleForECS

Descrizione: fornisce l'accesso a tutto il CodeDeploy servizio per eseguire un'implementazione ECS blu/green per tuo conto. Garantisce l'accesso completo ai servizi di supporto, come l'accesso completo per leggere tutti gli oggetti S3, richiamare tutte le funzioni Lambda, pubblicare su tutti gli argomenti SNS all'interno dell'account e aggiornare tutti i servizi ECS.

AWSCodeDeployRoleForECS [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSCodeDeployRoleForECS ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 20:40 UTC
- Ora modificata: 23 settembre 2019, 22:37 UTC

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

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployRoleForECSLimited

Descrizione: fornisce un accesso limitato al CodeDeploy servizio per eseguire un'implementazione ECS blu/green per tuo conto.

AWSCodeDeployRoleForECSLimited è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeDeployRoleForECSLimited ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 20:42 UTC
- Ora modificata: 23 settembre 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployRoleForLambda

Descrizione: fornisce l'accesso al CodeDeploy servizio per eseguire una distribuzione Lambda per tuo conto.

AWSCodeDeployRoleForLambda è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeDeployRoleForLambda ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 novembre 2017, 14:05 UTC
- Ora modificata: 03 dicembre 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeDeployRoleForLambdaLimited

Descrizione: fornisce un accesso limitato al CodeDeploy servizio per eseguire una distribuzione Lambda per tuo conto.

AWSCodeDeployRoleForLambdaLimited è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeDeployRoleForLambdaLimited ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 agosto 2020, 17:14 UTC
- Ora modificata: 17 agosto 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodePipeline_FullAccess

Descrizione: Fornisce l'accesso completo AWS CodePipeline tramite AWS Management Console.

AWSCodePipeline_FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodePipeline_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 agosto 2020, 22:38 UTC
- Ora modificata: 14 marzo 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodePipeline_ReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura AWS CodePipeline tramite AWS Management Console.

AWSCodePipeline_ReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodePipeline_ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 agosto 2020, 22:25 UTC
- Ora modificata: 03 agosto 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
    "codestar-notifications:DescribeNotificationRule"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
    }
  }
}
],
"Version" : "2012-10-17"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodePipelineApproverAccess

Descrizione: fornisce l'accesso per visualizzare e approvare le modifiche manuali per tutte le pipeline

AWSCodePipelineApproverAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodePipelineApproverAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 luglio 2016, 18:59 UTC
- Ora modificata: 02 agosto 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodePipelineCustomActionAccess

Descrizione: fornisce l'accesso ad azioni personalizzate per verificare i dettagli delle offerte di lavoro (incluse le credenziali temporanee) e segnalare gli aggiornamenti di stato. AWS CodePipeline

AWSCodePipelineCustomActionAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodePipelineCustomActionAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:02 UTC
- Ora modificata: 9 luglio 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeStarFullAccess

Descrizione: Fornisce l'accesso completo AWS CodeStar tramite AWS Management Console.

AWSCodeStarFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCodeStarFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 aprile 2017, 16:23 UTC
- Ora modificata: 28 marzo 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeStarNotificationsServiceRolePolicy

Descrizione: consente alle AWS CodeStar notifiche di accedere ad Amazon CloudWatch Events per tuo conto

AWSCodeStarNotificationsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 novembre 2019, 16:10 UTC
- Ora modificata: 19 marzo 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCodeStarServiceRole

Descrizione: DO NOT USE - AWS CodeStar Service Role Policy che concede privilegi amministrativi per CodeStar gestire IAM e altre risorse di servizio per conto del cliente.

AWSCodeStarServiceRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSCodeStarServiceRole` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 aprile 2017, 15:20 UTC
- Ora modificata: 20 settembre 2021, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCompromisedKeyQuarantine

Descrizione: nega l'accesso a determinate azioni, applicate dal AWS team nel caso in cui le credenziali di un utente IAM siano state compromesse o esposte pubblicamente. NON rimuovere questa politica. Segui invece le istruzioni specificate nell'e-mail che ti è stata inviata in merito a questo evento.

AWSCompromisedKeyQuarantine è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCompromisedKeyQuarantine ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 agosto 2020, 18:04 UTC
- Ora modificata: 11 agosto 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCompromisedKeyQuarantineV2

Descrizione: nega l'accesso a determinate azioni, applicate dal AWS team nel caso in cui le credenziali di un utente IAM siano state compromesse o esposte pubblicamente. **NON** rimuovere questa politica. Segui invece le istruzioni specificate nella richiesta di assistenza creata per te in merito a questo evento.

AWSCompromisedKeyQuarantineV2 è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSCompromisedKeyQuarantineV2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 aprile 2021, 22:30 UTC
- Ora modificata: 16 marzo 2023, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSConfigMultiAccountSetupPolicy

Descrizione: consente a Config di chiamare AWS i servizi e distribuire risorse di configurazione in tutta l'organizzazione

AWSConfigMultiAccountSetupPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 giugno 2019, 18:03 UTC
- Ora modificata: 24 febbraio 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSConfigRemediationServiceRolePolicy

Descrizione: consente a AWS Config di correggere le risorse non conformi per tuo conto.

AWSConfigRemediationServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 giugno 2019, 21:21 UTC
- Ora modificata: 18 giugno 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSConfigRoleForOrganizations

Descrizione: consente a AWS Config di chiamare le API Organizations di sola lettura AWS

AWSConfigRoleForOrganizations [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSConfigRoleForOrganizations ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 marzo 2018, 22:53 UTC
- Ora modificata: 24 novembre 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSConfigRulesExecutionRole

Descrizione: consente a una funzione AWS Lambda di accedere all'API AWS Config e agli snapshot di configurazione che Config AWS fornisce periodicamente ad Amazon S3. Questo accesso è richiesto dalle funzioni che valutano le modifiche alla configurazione per le regole di Config personalizzate.

AWSConfigRulesExecutionRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSConfigRulesExecutionRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 marzo 2016, 17:59 UTC
- Ora modificata: 13 maggio 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSConfigServiceRolePolicy

Descrizione: consente a Config di chiamare AWS i servizi e raccogliere le configurazioni delle risorse per tuo conto.

AWSConfigServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 maggio 2018, 23:31 UTC
- Ora modificata: 22 febbraio 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Versione della politica

Versione della politica: v50 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:GetEntityType",
"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/*"
  ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSConfigUserAccess

Descrizione: fornisce l'accesso all'utilizzo di AWS Config, inclusa la ricerca per tag sulle risorse e la lettura di tutti i tag. Ciò non fornisce l'autorizzazione per configurare AWS Config, che richiede privilegi amministrativi.

AWSConfigUserAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSConfigUserAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 febbraio 2015, 19:38 UTC
- Ora modificata: 18 marzo 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSConnector

Descrizione: consente un ampio accesso in lettura/scrittura a TUTTI gli oggetti EC2, l'accesso in lettura/scrittura ai bucket S3 che iniziano con «import-to-ec2-» e la possibilità di elencare tutti i bucket S3, affinché il Connector possa importare le VM per tuo conto. AWS

AWSConnector [è una policy gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSConnector ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 febbraio 2015, 17:14 UTC
- Ora modificata: 28 settembre 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:DescribeInstanceState",
        "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-*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSControlTowerAccountServiceRolePolicy

Descrizione: consente a AWS Control Tower di chiamare AWS servizi che forniscono la configurazione automatica degli account e la governance centralizzata per conto dell'utente.

AWSControlTowerAccountServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 giugno 2023, 22:04 UTC
- Ora modificata: 5 giugno 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSControlTowerServiceRolePolicy

Descrizione: Fornisce l'accesso alle AWS risorse gestite o utilizzate da AWS Control Tower

AWSControlTowerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSControlTowerServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 03 maggio 2019, 18:19 UTC
- Ora modificata: 12 aprile 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSCostAndUsageReportAutomationPolicy

Descrizione: concede le autorizzazioni per descrivere l'organizzazione dell'account, creare bucket S3 per il programma MAP e applicarvi tag, creare un rapporto sui costi e sull'utilizzo e descrivere le definizioni del rapporto sui costi e sull'utilizzo.

AWSCostAndUsageReportAutomationPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AWSCostAndUsageReportAutomationPolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 01 novembre 2021, 21:27 UTC
- Ora modificata: 01 novembre 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDataExchangeFullAccess

Descrizione: concede l'accesso completo a AWS Data Exchange e alle Marketplace AWS azioni utilizzando l'SDK AWS Management Console and. Fornisce inoltre un accesso selezionato ai servizi correlati necessari per sfruttare appieno il AWS Data Exchange.

AWSDataExchangeFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDataExchangeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 19:27 UTC
- Ora modificata: 07 maggio 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Sid" : "S3WriteActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource" : "arn:aws:s3::*aws-data-exchange*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "dataexchange.amazonaws.com"
        ]
      }
    }
  }
],
{
  "Sid" : "S3ReadActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
```

```

    "Sid" : "AWSMarketplaceProviderActions",
    "Effect" : "Allow",
    "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AWSMarketplaceSubscriberActions",
    "Effect" : "Allow",
    "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:GetPrivateListing",
        "aws-marketplace:DescribeAgreement"
    ],
    "Resource" : "*"
},
{
    "Sid" : "KMSActions",
    "Effect" : "Allow",
    "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",

```



```
        "kms:ListKeys"
    ],
    "Resource" : "*"
},
{
    "Sid" : "RedshiftConditionalActions",
    "Effect" : "Allow",
    "Action" : [
        "redshift:AuthorizeDataShare"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEqualsIgnoreCase" : {
            "redshift:ConsumerIdentifier" : "ADX"
        }
    }
},
{
    "Sid" : "RedshiftActions",
    "Effect" : "Allow",
    "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
    ],
    "Resource" : "*"
},
{
    "Sid" : "APIGatewayActions",
    "Effect" : "Allow",
    "Action" : [
        "apigateway:GET"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDDataExchangeProviderFullAccess

Descrizione: concede al provider di dati l'accesso a AWS Data Exchange e alle Marketplace AWS azioni utilizzando l'SDK AWS Management Console and. Fornisce inoltre un accesso selezionato ai servizi correlati necessari per sfruttare appieno il AWS Data Exchange.

AWSDDataExchangeProviderFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDDataExchangeProviderFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 19:27 UTC
- Ora modificata: 15 marzo 2022, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDDataExchangeProviderFullAccess`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDataExchangeReadOnly

Descrizione: concede l'accesso in sola lettura a AWS Data Exchange e alle Marketplace AWS azioni utilizzando l' AWS Management Console SDK and.

AWSDataExchangeReadOnly [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSDataExchangeReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 19:27 UTC
- Ora modificata: 10 maggio 2021, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDataExchangeSubscriberFullAccess

Descrizione: concede agli abbonati ai dati l'accesso a AWS Data Exchange e alle Marketplace AWS azioni utilizzando l'SDK AWS Management Console and. Fornisce inoltre un accesso selezionato ai servizi correlati necessari per sfruttare appieno il AWS Data Exchange.

AWSDataExchangeSubscriberFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDataExchangeSubscriberFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 19:27 UTC
- Ora modificata: 21 maggio 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "DataExchangeReadOnlyActions",
    "Effect" : "Allow",
    "Action" : [
      "dataexchange:Get*",
      "dataexchange:List*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DataExchangeExportActions",
    "Effect" : "Allow",
    "Action" : [
      "dataexchange:CreateJob",
      "dataexchange:StartJob",
      "dataexchange:CancelJob"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "dataexchange:JobType" : [
          "EXPORT_ASSETS_TO_S3",
          "EXPORT_ASSET_TO_SIGNED_URL",
          "EXPORT_REVISIONS_TO_S3"
        ]
      }
    }
  },
  {
    "Sid" : "DataExchangeEventActionActions",
    "Effect" : "Allow",
    "Action" : [
      "dataexchange:CreateEventAction",
      "dataexchange:UpdateEventAction",
      "dataexchange>DeleteEventAction",
      "dataexchange:SendApiAsset"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "S3GetActionConditionalResourceAndADX",
    "Effect" : "Allow",
```

```
"Action" : "s3:GetObject",
"Resource" : "arn:aws:s3::*aws-data-exchange*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "dataexchange.amazonaws.com"
    ]
  }
},
{
  "Sid" : "S3ReadActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSMarketplaceSubscriberActions",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:Subscribe",
    "aws-marketplace:Unsubscribe",
    "aws-marketplace:ViewSubscriptions",
    "aws-marketplace:GetAgreementRequest",
    "aws-marketplace:ListAgreementRequests",
    "aws-marketplace:CancelAgreementRequest",
    "aws-marketplace:ListPrivateListings"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KMSActions",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:ListKeys"
  ],
  "Resource" : "*"
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDatalifecycleManagerServiceRole

Descrizione: fornisce le autorizzazioni appropriate a AWS Data Lifecycle Manager per intraprendere azioni sulle risorse AWS

AWSDatalifecycleManagerServiceRole è [una policy gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSDatalifecycleManagerServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 luglio 2018, 19:34 UTC
- Ora modificata: 19 settembre 2022, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDatalifecycleManagerServiceRole`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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.*"  
  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDatalifecycleManagerServiceRoleForAMIManagement

Descrizione: Fornisce le autorizzazioni appropriate a AWS Data Lifecycle Manager per intraprendere azioni sulle risorse AWS per la gestione delle AMI

AWSDatalifecycleManagerServiceRoleForAMIManagement [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSDatalifecycleManagerServiceRoleForAMIManagement ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 21 ottobre 2020, 19:39 UTC
- Ora modificata: 19 agosto 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDataLifecycleManagerSSMFullAccess

Descrizione: fornisce ad Amazon Data Lifecycle Manager l'autorizzazione a eseguire le azioni di Systems Manager necessarie per eseguire script pre e post su tutte le istanze Amazon EC2.

AWSDataLifecycleManagerSSMFullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSDataLifecycleManagerSSMFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 31 ottobre 2023, 20:29 UTC
- Ora modificata: 16 novembre 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDatapipeline_FullAccess

Descrizione: fornisce accesso completo a Data Pipeline, accesso alle liste per i ruoli S3, DynamoDB, Redshift, RDS, SNS e IAM e accesso PassRole per i ruoli predefiniti.

AWSDatapipeline_FullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSDatapipeline_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 gennaio 2017, 23:14 UTC
- Ora modificata: 17 agosto 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDataPipeline_PowerUser

Descrizione: fornisce accesso completo a Data Pipeline, accesso alle liste per i ruoli S3, DynamoDB, Redshift, RDS, SNS e IAM e accesso PassRole per i ruoli predefiniti.

AWSDataPipeline_PowerUser [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSDataPipeline_PowerUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 gennaio 2017, 23:16 UTC
- Ora modificata: 17 agosto 2017, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDDataSyncDiscoveryServiceRolePolicy

Descrizione: consente a DataSync Discovery di integrarsi con altri AWS servizi per conto dell'utente.

AWSDDataSyncDiscoveryServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 marzo 2023, 22:19 UTC
- Ora modificata: 20 marzo 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDDataSyncDiscoveryServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDDataSyncFullAccess

Descrizione: fornisce accesso completo AWS DataSync e accesso minimo alle sue dipendenze

AWSDDataSyncFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDDataSyncFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2019, 19:40 UTC
- Ora modificata: 16 febbraio 2024, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDDataSyncFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
}

```



```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDDataSyncReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a AWS DataSync

AWSDDataSyncReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDDataSyncReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2019, 19:18 UTC
- Ora modificata: 30 giugno 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDDataSyncReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeadlineCloud-FleetWorker

Descrizione: fornisce ai lavoratori di AWS Deadline Cloud l'accesso all'esecuzione delle attività in una fattoria.

AWSDeadlineCloud-FleetWorker è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSDeadlineCloud-FleetWorker` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:21 UTC
- Ora modificata: 01 aprile 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunTasksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForWorker",
        "deadline:UpdateWorker",
        "deadline:UpdateWorkerSchedule",
        "deadline:BatchGetJobEntity",
        "deadline:AssumeQueueRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeadlineCloud-UserAccessFarms

Descrizione: fornisce l'accesso alla workstation utente alle farm AWS Deadline Cloud con autorizzazioni di sola lettura limitate per chiamare altri servizi necessari. Allega questa policy al ruolo utente associato al tuo studio.

AWSDeadlineCloud-UserAccessFarms è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeadlineCloud-UserAccessFarms ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 16:54 UTC
- Ora modificata: 01 aprile 2024, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline>CreateBudget",
        "deadline>DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
        "deadline:GetBudget",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:ListBudgets",
        "deadline:StartSessionsStatisticsAggregation",
        "deadline:UpdateBudget"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```

    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:FarmMembershipLevels" : [
          "OWNER"
        ]
      }
    },
  },
  {
    "Sid" : "ManagerLevelMemberAssociation",
    "Effect" : "Allow",
    "Action" : [
      "deadline:AssociateMemberToFarm",
      "deadline:AssociateMemberToFleet",
      "deadline:AssociateMemberToJob",
      "deadline:AssociateMemberToQueue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:FarmMembershipLevels" : [
          "MANAGER"
        ]
      },
      "StringEquals" : {
        "deadline:AssociatedMembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER",
          ""
        ],
        "deadline:MembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER"
        ]
      }
    }
  },
  {
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",

```

```

    "Action" : [
      "deadline:DisassociateMemberFromFarm",
      "deadline:DisassociateMemberFromFleet",
      "deadline:DisassociateMemberFromJob",
      "deadline:DisassociateMemberFromQueue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:FarmMembershipLevels" : [
          "MANAGER"
        ]
      },
      "StringEquals" : {
        "deadline:AssociatedMembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER",
          ""
        ]
      }
    }
  },
  {
    "Sid" : "OwnerManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "deadline:ListFarmMembers",
      "deadline:ListFleetMembers",
      "deadline:ListJobMembers",
      "deadline:ListQueueMembers",
      "deadline:UpdateJob",
      "deadline:UpdateSession",
      "deadline:UpdateStep",
      "deadline:UpdateTask"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:FarmMembershipLevels" : [

```

```

        "OWNER",
        "MANAGER"
    ]
}
},
{
    "Sid" : "OwnerManagerContributorPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:FarmMembershipLevels" : [
                "OWNER",
                "MANAGER",
                "CONTRIBUTOR"
            ]
        }
    }
},
{
    "Sid" : "AllLevelsPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",

```



```

        "deadline:GetWorker",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:FarmMembershipLevels" : [
                "OWNER",
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER"
            ]
        }
    }
},
{
    "Sid" : "ListBasedOnMembership",
    "Effect" : "Allow",
    "Action" : [
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListQueues"
    ],
    "Resource" : [
        "*"
    ],

```

```
"Condition" : {
  "StringEquals" : {
    "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeadlineCloud-UserAccessFleets

Descrizione: fornisce l'accesso alla workstation utente alle flotte di AWS Deadline Cloud con autorizzazioni di sola lettura limitate per chiamare altri servizi necessari. Allega questa policy al ruolo utente associato al tuo studio.

AWSDeadlineCloud-UserAccessFleets è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeadlineCloud-UserAccessFleets ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:01 UTC
- Ora modificata: 01 aprile 2024, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet",
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    }
  ],
  {
```

```

    "Sid" : "ManagerLevelMemberAssociation",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssociateMemberToFleet"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:FleetMembershipLevels" : [
                "MANAGER"
            ]
        },
        "StringEquals" : {
            "deadline:AssociatedMembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER",
                ""
            ],
            "deadline:MembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER"
            ]
        }
    },
},
{
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",
    "Action" : [
        "deadline:DisassociateMemberFromFleet"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:FleetMembershipLevels" : [
                "MANAGER"
            ]
        }
    },
},

```

```

        "StringEquals" : {
            "deadline:AssociatedMembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER",
                ""
            ]
        }
    },
    {
        "Sid" : "OwnerManagerPermissions",
        "Effect" : "Allow",
        "Action" : [
            "deadline:ListFleetMembers"
        ],
        "Resource" : [
            "*"
        ],
        "Condition" : {
            "ForAnyValue:StringEquals" : {
                "deadline:FleetMembershipLevels" : [
                    "OWNER",
                    "MANAGER"
                ]
            }
        }
    },
    {
        "Sid" : "AllLevelsPermissions",
        "Effect" : "Allow",
        "Action" : [
            "deadline:AssumeFleetRoleForRead",
            "deadline:GetFleet",
            "deadline:GetQueueFleetAssociation",
            "deadline:GetWorker",
            "deadline:ListQueueFleetAssociations",
            "deadline:ListSessionsForWorker",
            "deadline:ListWorkers",
            "deadline:SearchWorkers"
        ],
        "Resource" : [
            "*"
        ]
    },

```

```
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "deadline:FleetMembershipLevels" : [
      "OWNER",
      "MANAGER",
      "CONTRIBUTOR",
      "VIEWER"
    ]
  }
},
{
  "Sid" : "ListBasedOnMembership",
  "Effect" : "Allow",
  "Action" : [
    "deadline:ListFleets"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeadlineCloud-UserAccessJobs

Descrizione: fornisce all'utente l'accesso alla workstation ai job di AWS Deadline Cloud con autorizzazioni di sola lettura limitate per chiamare altri servizi necessari. Allega questa policy al ruolo utente associato al tuo studio.

AWSDeadlineCloud-UserAccessJobs è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeadlineCloud-UserAccessJobs ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:05 UTC
- Ora modificata: 01 aprile 2024, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",

```

```

        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "OwnerLevelPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromJob"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:JobMembershipLevels" : [
                "OWNER"
            ]
        }
    }
},
{
    "Sid" : "ManagerLevelMemberAssociation",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssociateMemberToJob"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:JobMembershipLevels" : [
                "MANAGER"
            ]
        },
        "StringEquals" : {
            "deadline:AssociatedMembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",

```



```

        "VIEWER",
        ""
    ],
    "deadline:MembershipLevel" : [
        "MANAGER",
        "CONTRIBUTOR",
        "VIEWER"
    ]
}
},
{
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",
    "Action" : [
        "deadline:DisassociateMemberFromJob"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:JobMembershipLevels" : [
                "MANAGER"
            ]
        },
        "StringEquals" : {
            "deadline:AssociatedMembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER",
                ""
            ]
        }
    }
},
{
    "Sid" : "OwnerManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:ListJobMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",

```

```

        "deadline:UpdateTask"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:JobMembershipLevels" : [
                "OWNER",
                "MANAGER"
            ]
        }
    }
},
{
    "Sid" : "AllLevelsPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:GetJob",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetTask",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListTasks",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:JobMembershipLevels" : [
                "OWNER",
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER"
            ]
        }
    }
}

```

```
    }
  },
  {
    "Sid" : "ListBasedOnMembership",
    "Effect" : "Allow",
    "Action" : [
      "deadline:ListJobs"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeadlineCloud-UserAccessQueues

Descrizione: fornisce all'utente l'accesso alla workstation alle code di AWS Deadline Cloud con autorizzazioni di sola lettura limitate per chiamare altri servizi necessari. Allega questa policy al ruolo utente associato al tuo studio.

AWSDeadlineCloud-UserAccessQueues è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeadlineCloud-UserAccessQueues ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:10 UTC
- Ora modificata: 01 aprile 2024, 17:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
```

```

        "deadline:AssociateMemberToQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:QueueMembershipLevels" : [
                "OWNER"
            ]
        }
    }
},
{
    "Sid" : "ManagerLevelMemberAssociation",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:QueueMembershipLevels" : [
                "MANAGER"
            ]
        },
        "StringEquals" : {
            "deadline:AssociatedMembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER",
                ""
            ],
            "deadline:MembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER"
            ]
        }
    }
}

```

```

    }
  },
  {
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",
    "Action" : [
      "deadline:DisassociateMemberFromJob",
      "deadline:DisassociateMemberFromQueue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:QueueMembershipLevels" : [
          "MANAGER"
        ]
      },
      "StringEquals" : {
        "deadline:AssociatedMembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER",
          ""
        ]
      }
    }
  },
  {
    "Sid" : "OwnerManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "deadline:ListJobMembers",
      "deadline:ListQueueMembers",
      "deadline:UpdateJob",
      "deadline:UpdateSession",
      "deadline:UpdateStep",
      "deadline:UpdateTask"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {

```

```

        "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER"
        ]
    }
},
{
    "Sid" : "OwnerManagerContributorPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline>CreateJob"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:QueueMembershipLevels" : [
                "OWNER",
                "MANAGER",
                "CONTRIBUTOR"
            ]
        }
    }
},
{
    "Sid" : "AllLevelsPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetJob",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",

```

```

        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:QueueMembershipLevels" : [
                "OWNER",
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER"
            ]
        }
    }
},
{
    "Sid" : "ListBasedOnMembership",
    "Effect" : "Allow",
    "Action" : [
        "deadline:ListJobs",
        "deadline:ListQueues"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
    }
}
]
}

```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeadlineCloud-WorkerHost

Descrizione: consente agli host di lavoratori di AWS Deadline Cloud di entrare a far parte di una flotta in una fattoria.

AWSDeadlineCloud-WorkerHost è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeadlineCloud-WorkerHost ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:28 UTC
- Ora modificata: 01 aprile 2024, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Sid" : "JoinFleetPermissions",
    "Effect" : "Allow",
    "Action" : [
      "deadline:CreateWorker",
      "deadline:AssumeFleetRoleForWorker"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeepLensLambdaFunctionAccessPolicy

Descrizione: questa politica specifica le autorizzazioni richieste dalle funzioni lambda DeepLens amministrative eseguite su un dispositivo DeepLens

AWSDeepLensLambdaFunctionAccessPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSDeepLensLambdaFunctionAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 15:47 UTC

- Ora modificata: 11 giugno 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeepLensServiceRolePolicy

Descrizione: concede AWS DeepLens l'accesso alle risorse e ai ruoli necessari e alle relative dipendenze Servizi AWS, tra cui IoT, S3 e GreenGrass Lambda DeepLens . AWS

AWSDeepLensServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSDeepLensServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 novembre 2017, 15:46 UTC
- Ora modificata: 25 settembre 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeepRacerAccountAdminAccess

Descrizione: accesso DeepRacer amministrativo a tutte le azioni, inclusa la commutazione tra la modalità multiutente e quella a utente singolo.

AWSDeepRacerAccountAdminAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSDeepRacerAccountAdminAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 28 ottobre 2021, 01:27 UTC
- Ora modificata: 28 ottobre 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeepRacerCloudFormationAccessPolicy

Descrizione: consente di CloudFormation creare e gestire AWS pile e risorse per tuo conto.

AWSDeepRacerCloudFormationAccessPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeepRacerCloudFormationAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 febbraio 2019, 21:59 UTC
- Ora modificata: 14 giugno 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    ]
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeepRacerDefaultMultiUserAccess

Descrizione: accesso utente DeepRacer MultiUser predefinito per utilizzare deepracer in modalità multiutente

AWSDeepRacerDefaultMultiUserAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti `AWSDeepRacerDefaultMultiUserAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 ottobre 2021, 01:27 UTC
- Ora modificata: 28 ottobre 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeepRacerFullAccess

Descrizione: Fornisce accesso completo a AWS DeepRacer. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3).

AWSDeepRacerFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeepRacerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 ottobre 2020, 22:03 UTC
- Ora modificata: 5 ottobre 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*/*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeepRacerRoboMakerAccessPolicy

Descrizione: consente di RoboMaker creare le risorse necessarie e chiamare AWS i servizi per conto dell'utente.

AWSDeepRacerRoboMakerAccessPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeepRacerRoboMakerAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 febbraio 2019, 21:59 UTC
- Ora modificata: 28 febbraio 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeepRacerServiceRolePolicy

Descrizione: consente di DeepRacer creare le risorse necessarie e chiamare AWS i servizi per conto dell'utente.

AWSDeepRacerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSDeepRacerServiceRolePolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 febbraio 2019, 21:58 UTC
- Ora modificata: 12 giugno 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDenyAll

Descrizione: nega tutti gli accessi.

AWSDenyAll è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDenyAll ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 maggio 2019, 22:36 UTC
- Ora modificata: 18 dicembre 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeviceFarmFullAccess

Descrizione: Fornisce l'accesso completo a tutte le operazioni di AWS Device Farm.

AWSDeviceFarmFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDeviceFarmFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 luglio 2015, 16:37 UTC
- Ora modificata: 13 luglio 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeviceFarmServiceRolePolicy

Descrizione: concedi le autorizzazioni a AWS Device Farm per chiamare le API di rete EC2 per tuo conto.

AWSDeviceFarmServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 settembre 2022, 21:02 UTC
- Ora modificata: 20 settembre 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]

```

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDeviceFarmTestGridServiceRolePolicy

Descrizione: concedi le autorizzazioni a AWS Device Farm per chiamare le API EC2 per tuo conto.

AWSDeviceFarmTestGridServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 maggio 2021, 22:01 UTC
- Ora modificata: 26 maggio 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDirectConnectFullAccess

Descrizione: Fornisce l'accesso completo a AWS Direct Connect tramite AWS Management Console.

AWSDirectConnectFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDirectConnectFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 30 aprile 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    "directconnect:*",
    "ec2:DescribeVpnGateways",
    "ec2:DescribeTransitGateways"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDirectConnectReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura a AWS Direct Connect tramite AWS Management Console.

AWSDirectConnectReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDirectConnectReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 18 maggio 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDirectConnectServiceRolePolicy

Descrizione: Fornisce l'autorizzazione AWS Direct Connect per creare e gestire AWS risorse per tuo conto.

AWSDirectConnectServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 gennaio 2021, 18:35 UTC
- Ora modificata: 14 gennaio 2021, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```


Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDirectoryServiceFullAccess

Descrizione: fornisce l'accesso completo a AWS Directory Service.

AWSDirectoryServiceFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDirectoryServiceFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 02 aprile 2024, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```

    "Action" : [
      "ds:*",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:DescribeSecurityGroups",
      "sns:GetTopicAttributes",
      "sns:ListSubscriptions",
      "sns:ListSubscriptionsByTopic",
      "sns:ListTopics",
      "iam:ListRoles",
      "organizations:ListAccountsForParent",
      "organizations:ListRoots",
      "organizations:ListAccounts",
      "organizations:DescribeOrganization",
      "organizations:DescribeAccount",
      "organizations:ListOrganizationalUnitsForParent",
      "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DirectoryServiceEventTopic",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns>DeleteTopic",
      "sns:SetTopicAttributes",
      "sns:Subscribe",
      "sns:Unsubscribe"
    ],
    "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
  },
  {
    "Sid" : "DirectoryServiceOrganizations",
    "Effect" : "Allow",

```

```
"Action" : [
  "organizations:EnableAWSServiceAccess",
  "organizations:DisableAWSServiceAccess"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "organizations:ServicePrincipal" : "ds.amazonaws.com"
  }
},
{
  "Sid" : "DirectoryServiceTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDirectoryServiceReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al AWS Directory Service.

AWSDirectoryServiceReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSDirectoryServiceReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 25 settembre 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDiscoveryContinuousExportFirehosePolicy

Descrizione: fornisce accesso in scrittura alle AWS risorse necessarie per AWS Discovery Continuous Export

AWSDiscoveryContinuousExportFirehosePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSDiscoveryContinuousExportFirehosePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 agosto 2018, 18:29 UTC
- Ora modificata: 08 giugno 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDMSFleetAdvisorServiceRolePolicy

Descrizione: consente a DMS Fleet Advisor di gestire le CloudWatch metriche per tuo conto.

AWSDMSFleetAdvisorServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 6 marzo 2023, 09:10 UTC
- Ora modificata: 6 marzo 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSDMSServerlessServiceRolePolicy

Descrizione: concede le autorizzazioni AWS DMS Serverless per creare e gestire le risorse DMS del tuo account per tuo conto

AWSDMSServerlessServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 maggio 2023, 20:28 UTC
- Ora modificata: 18 maggio 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
    ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSEC2CapacityReservationFleetRolePolicy

Descrizione: consente al servizio EC2 CapacityReservation Fleet di gestire le prenotazioni di capacità

AWSEC2CapacityReservationFleetRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 29 settembre 2021, 14:43 UTC
- Ora modificata: 29 settembre 2021, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSEC2FleetServiceRolePolicy

Descrizione: consente a EC2 Fleet di avviare e gestire le istanze.

AWSEC2FleetServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 marzo 2018, 00:08 UTC
- Ora modificata: 04 maggio 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
    ]
}
```

```
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSEC2SpotFleetServiceRolePolicy

Descrizione: consente a EC2 Spot Fleet di avviare e gestire le istanze del parco istanze spot

AWSEC2SpotFleetServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 ottobre 2017, 19:13 UTC
- Ora modificata: 16 marzo 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*/*"
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSEC2SpotServiceRolePolicy

Descrizione: consente a EC2 Spot di avviare e gestire istanze spot

AWSEC2SpotServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 settembre 2017, 18:51 UTC
- Ora modificata: 12 dicembre 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSEC2VssSnapshotPolicy

Descrizione: questa policy è associata al ruolo IAM associato alle istanze Windows di Amazon EC2 per consentire alla soluzione Amazon EC2 VSS di creare e aggiungere tag ad Amazon Machine Images (AMI) e agli snapshot EBS.

AWSEC2VssSnapshotPolicy è una [politica](#) gestita AWS.

Utilizzo di questa politica

Puoi collegarti AWSEC2VssSnapshotPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 marzo 2024, 16:32 UTC
- Ora modificata: 27 marzo 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:RequestTag/AwsVssConfig" : "*"
        }
    }
},
{
    "Sid" : "CreateSnapshotsAccessInstance",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateSnapshots"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "StringLike" : {
            "ec2:SourceInstanceARN" : "${ec2:InstanceId}"
        }
    }
},
{
    "Sid" : "CreateSnapshotsAccessVolume",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateSnapshots"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
    ]
},
{
    "Sid" : "CreateImageWithTag",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateImage"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
    ]
}

```

```

    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AwsVssConfig" : "*"
      }
    }
  },
  {
    "Sid" : "CreateImageAccessInstance",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateImage"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
      }
    }
  },
  {
    "Sid" : "CreateTagsOnResourceCreation",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateImage",
          "CreateSnapshots"
        ]
      }
    }
  },
  {
    "Sid" : "CreateTagsAfterResourceCreation",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [

```

```

    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:image/*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/AwsVssConfig" : "*"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AppConsistent",
        "Device"
      ]
    }
  }
},
{
  "Sid" : "DescribeImagesAndSnapshots",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeImages",
    "ec2:DescribeSnapshots"
  ],
  "Resource" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSECRPullThroughCache_ServiceRolePolicy

Descrizione: consente l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da AWS ECR pull through cache

AWSECRPullThroughCache_ServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 novembre 2021, 21:51 UTC
- Ora modificata: 13 novembre 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
    }
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

Descrizione: autorizza l'istanza nel tuo ambiente di creazione di piattaforme personalizzate ad avviare un'istanza EC2, creare snapshot e AMI EBS, trasmettere i log ad Amazon Logs e archiviare artefatti in CloudWatch Amazon S3.

AWSElasticBeanstalkCustomPlatformforEC2Role [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkCustomPlatformforEC2Role ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 febbraio 2017, 22:50 UTC
- Ora modificata: 21 febbraio 2017, 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkEnhancedHealth

Descrizione: politica di AWS Elastic Beanstalk Service per il sistema di monitoraggio della salute

AWSElasticBeanstalkEnhancedHealth [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkEnhancedHealth ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 8 febbraio 2016, 23:17 UTC
- Ora modificata: 09 aprile 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkMaintenance

Descrizione: AWS politica del ruolo del servizio Elastic Beanstalk che concede autorizzazioni limitate per aggiornare le risorse per tuo conto a fini di manutenzione.

AWSElasticBeanstalkMaintenance [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 11 gennaio 2019, 23:22 UTC
- Ora modificata: 29 aprile 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ]
    }
  ],
```

```
"Resource" : [
  "arn:aws:cloudformation:*:*:stack/awseb-*",
  "arn:aws:cloudformation:*:*:stack/eb-*"
],
{
  "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DescribeLoadBalancers",
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Descrizione: questa policy riguarda il ruolo del servizio AWS Elastic Beanstalk utilizzato per eseguire aggiornamenti gestiti degli ambienti Elastic Beanstalk. Questa politica non deve essere associata ad altri utenti o ruoli. La policy concede ampie autorizzazioni per creare e gestire risorse su una serie di AWS servizi AutoScaling, tra cui EC2, ECS, Elastic Load Balancing e. CloudFormation Questa policy consente inoltre il trasferimento di qualsiasi ruolo IAM utilizzabile con tali servizi.

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 3 marzo 2021, 22:18 UTC
- Ora modificata: 23 marzo 2023, 23:15 UTC

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

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "CFN0perationPermissions",
    "Effect" : "Allow",
    "Action" : [
        "cloudformation:*"
    ],
    "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
    ]
},
{
    "Sid" : "ELB0perationPermissions",
    "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" : "CWLogs0perationPermissions",
    "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"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Descrizione: AWS politica del ruolo del servizio Elastic Beanstalk che concede autorizzazioni limitate agli aggiornamenti gestiti.

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 novembre 2019, 22:35 UTC
- Ora modificata: 29 aprile 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```

    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "iam:PassedToService" : [
          "elasticbeanstalk.amazonaws.com",
          "ec2.amazonaws.com",
          "autoscaling.amazonaws.com",
          "elasticloadbalancing.amazonaws.com",
          "ecs.amazonaws.com",
          "cloudformation.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "SingleInstanceAPIs",
    "Effect" : "Allow",
    "Action" : [
      "ec2:releaseAddress",
      "ec2:allocateAddress",
      "ec2:DisassociateAddress",
      "ec2:AssociateAddress"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ECS",
    "Effect" : "Allow",
    "Action" : [
      "ecs:RegisterTaskDefinition",
      "ecs:DeRegisterTaskDefinition",
      "ecs:List*",
      "ecs:Describe*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ElasticBeanstalkAPIs",
    "Effect" : "Allow",
    "Action" : [
      "elasticbeanstalk:*"
    ]
  },

```

```

    "Resource" : "*"
  },
  {
    "Sid" : "ReadOnlyAPIs",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:Describe*",
      "cloudformation:List*",
      "ec2:Describe*",
      "autoscaling:Describe*",
      "elasticloadbalancing:Describe*",
      "logs:DescribeLogGroups",
      "sns:GetTopicAttributes",
      "sns:ListSubscriptionsByTopic",
      "rds:DescribeDBEngineVersions",
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ASG",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling:CreateOrUpdateTags",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling>DeleteScheduledAction",
      "autoscaling:DetachInstances",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:PutScalingPolicy",
      "autoscaling:PutScheduledUpdateGroupAction",
      "autoscaling:ResumeProcesses",
      "autoscaling:SuspendProcesses",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "autoscaling:UpdateAutoScalingGroup"
    ],
    "Resource" : [
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",

```

```

        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
    ]
},
{
    "Sid" : "CFN",
    "Effect" : "Allow",
    "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation>DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
    ],
    "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
    ]
},
{
    "Sid" : "EC2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringLike" : {
            "ec2:ResourceTag/aws:cloudformation:stack-id" : [
                "arn:aws:cloudformation:*:*:stack/awseb-e-*",
                "arn:aws:cloudformation:*:*:stack/eb-*"
            ]
        }
    }
},
{
    "Sid" : "S3obj",
    "Effect" : "Allow",
    "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",

```

```

        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
    ],
    "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
},
{
    "Sid" : "S3Bucket",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
    ],
    "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
},
{
    "Sid" : "CWL",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
},
{
    "Sid" : "ELB",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
    ],
    "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
    ]
},

```

```
{
  "Sid" : "SNS",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic"
  ],
  "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
},
{
  "Sid" : "EC2LaunchTemplate",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate",
    "ec2:DeleteLaunchTemplate",
    "ec2:CreateLaunchTemplateVersion",
    "ec2:DeleteLaunchTemplateVersions"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*"
},
{
  "Sid" : "AllowLaunchTemplateRunInstances",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "AllowECSTagResource",
  "Effect" : "Allow",
  "Action" : [
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:CreateAction" : [
        "RegisterTaskDefinition"
      ]
    }
  }
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkMulticontainerDocker

Descrizione: fornisci alle istanze del tuo ambiente Docker multicontainer l'accesso per utilizzare Amazon EC2 Container Service per gestire le attività di distribuzione dei container.

AWSElasticBeanstalkMulticontainerDocker [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkMulticontainerDocker ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 febbraio 2016, 23:15 UTC
- Ora modificata: 23 marzo 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkReadOnly

Descrizione: concede autorizzazioni di sola lettura. Consente esplicitamente agli operatori di ottenere l'accesso diretto per recuperare informazioni sulle risorse relative alle applicazioni Elastic AWS Beanstalk.

AWSElasticBeanstalkReadOnly [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 gennaio 2021, 19:02 UTC
- Ora modificata: 22 gennaio 2021, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkRoleCore

Descrizione: AWSElasticBeanstalkRoleCore (ruolo operativo Elastic Beanstalk) Consente il funzionamento principale di un ambiente di servizi Web.

AWSElasticBeanstalkRoleCore [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkRoleCore ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:48 UTC
- Ora modificata: 30 aprile 2024, 00:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
},
{
    "Sid" : "CloudWatch",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
    ]
}

```

```

    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
  },
  {
    "Sid" : "ELB",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:Create*",
      "elasticloadbalancing>Delete*",
      "elasticloadbalancing:Modify*",
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:DeRegisterTargets",
      "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
      "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
      "elasticloadbalancing:*Tags",
      "elasticloadbalancing:ConfigureHealthCheck",
      "elasticloadbalancing:SetRulePriorities",
      "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
      "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
    ]
  },
  {
    "Sid" : "ListAPIs",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:Describe*",
      "cloudformation:Describe*",
      "logs:Describe*",
      "ec2:Describe*",
      "ecs:Describe*",
      "ecs:List*",
      "elasticloadbalancing:Describe*",
      "rds:Describe*",
      "sns:List*",
      "iam:List*",

```

```

        "acm:Describe*",
        "acm:List*"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowPassRole",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "elasticbeanstalk.amazonaws.com",
                "ec2.amazonaws.com",
                "autoscaling.amazonaws.com",
                "elasticloadbalancing.amazonaws.com",
                "ecs.amazonaws.com",
                "cloudformation.amazonaws.com"
            ]
        }
    }
}
]
}
}
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkRoleCWL

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un ambiente di gestire CloudWatch i gruppi di log di Amazon Logs.

AWSElasticBeanstalkRoleCWL [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AWSElasticBeanstalkRoleCWL` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:49 UTC
- Ora modificata: 5 giugno 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkRoleECS

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un ambiente Docker multicontainer di gestire i cluster Amazon ECS.

AWSElasticBeanstalkRoleECS [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkRoleECS ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:47 UTC
- Ora modificata: 23 marzo 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkRoleRDS

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un ambiente di integrare un'istanza Amazon RDS.

AWSElasticBeanstalkRoleRDS [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkRoleRDS ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:46 UTC
- Ora modificata: 5 giugno 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkRoleSNS

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un ambiente di abilitare l'integrazione degli argomenti di Amazon SNS.

AWSElasticBeanstalkRoleSNS [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkRoleSNS ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:46 UTC
- Ora modificata: 5 giugno 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkRoleWorkerTier

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un livello di ambiente di lavoro di creare una tabella Amazon DynamoDB e una coda Amazon SQS.

AWSElasticBeanstalkRoleWorkerTier [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkRoleWorkerTier ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:43 UTC
- Ora modificata: 5 giugno 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkService

Descrizione: questa politica si trova su un percorso obsoleto. Consulta la documentazione come guida: <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>. AWS Politica del ruolo di Elastic Beanstalk Service che concede le autorizzazioni per creare e gestire risorse (AutoScalingad esempio: EC2, CloudFormation S3, ELB, ecc.) per tuo conto.

AWSElasticBeanstalkService [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkService ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio

- Ora di creazione: 11 aprile 2016, 20:27 UTC
- Ora modificata: 10 maggio 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Versione della politica

Versione della politica: v17 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkServiceRolePolicy

Descrizione: politica AWS Elastic Beanstalk Service Linked Role che concede le autorizzazioni per creare e gestire risorse (AutoScalingad esempio: EC2, CloudFormation S3, ELB, ecc.) per tuo conto.

AWSElasticBeanstalkServiceRolePolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 settembre 2017, 23:46 UTC
- Ora modificata: 6 giugno 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkWebTier

Descrizione: fornisci alle istanze del tuo ambiente server Web l'accesso per caricare file di registro su Amazon S3.

AWSElasticBeanstalkWebTier è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkWebTier ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 febbraio 2016, 23:08 UTC
- Ora modificata: 09 settembre 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticBeanstalkWorkerTier

Descrizione: consenti alle istanze del tuo ambiente di lavoro di accedere per caricare file di log su Amazon S3, usare Amazon SQS per monitorare la coda di lavoro della tua applicazione, usare Amazon DynamoDB per eleggere i leader e Amazon per pubblicare metriche per il monitoraggio dello stato. CloudWatch

AWSElasticBeanstalkWorkerTier [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticBeanstalkWorkerTier ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 febbraio 2016, 23:12 UTC
- Ora modificata: 09 settembre 2020, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryAgentInstallationPolicy

Descrizione: questa policy consente di installare il AWS Replication Agent, che viene utilizzato con AWS Elastic Disaster Recovery (DRS) per ripristinare i server esterni. AWS Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante la fase di installazione dell'agente di replica. AWS

AWSElasticDisasterRecoveryAgentInstallationPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryAgentInstallationPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2021, 10:37 UTC
- Ora modificata: 27 novembre 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryAgentPolicy

Descrizione: questa policy consente di utilizzare il AWS Replication Agent, utilizzato con AWS Elastic Disaster Recovery (DRS) per ripristinare i server di origine. AWS Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

AWSElasticDisasterRecoveryAgentPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSElasticDisasterRecoveryAgentPolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 10:32 UTC
- Ora modificata: 27 novembre 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryConsoleFullAccess

Descrizione: questa policy fornisce l'accesso completo a tutte le API pubbliche di AWS Elastic Disaster Recovery (DRS), nonché le autorizzazioni per leggere le informazioni su KMS key, License Manager, Resource Groups, Elastic Load Balancing, IAM ed EC2. Allega questa policy ai tuoi utenti o ruoli IAM.

AWSElasticDisasterRecoveryConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2021, 10:46 UTC
- Ora modificata: 16 ottobre 2023, 12:24 UTC

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

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
```

```

        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ConsoleFullAccess4",
    "Effect" : "Allow",
    "Action" : "license-manager:ListLicenseConfigurations",
    "Resource" : "*"
},
{
    "Sid" : "ConsoleFullAccess5",
    "Effect" : "Allow",
    "Action" : "resource-groups:ListGroups",
    "Resource" : "*"
},
{
    "Sid" : "ConsoleFullAccess6",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
},
{
    "Sid" : "ConsoleFullAccess7",
    "Effect" : "Allow",
    "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
    ],
    "Resource" : "*"
},
{

```

```

    "Sid" : "ConsoleFullAccess8",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2::*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess10",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2:DeleteLaunchTemplateVersions",
      "ec2:CreateTags",
      "ec2:DeleteTags"
    ],
    "Resource" : "arn:aws:ec2::*:launch-template/*",
    "Condition" : {
      "Null" : {

```

```
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
}
},
{
    "Sid" : "ConsoleFullAccess11",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
    }
},
{
    "Sid" : "ConsoleFullAccess12",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
            "aws:ViaAWSService" : "true"
        }
    }
},
{
    "Sid" : "ConsoleFullAccess13",
    "Effect" : "Allow",
    "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
    ],
}
```

```

    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess14",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess15",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  }
},

```

```
{
  "Sid" : "ConsoleFullAccess16",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSecurityGroup",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "ConsoleFullAccess17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess18",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess19",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
```

```

    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess20",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume",
      "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess21",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume",
      "ec2:AttachVolume",
      "ec2:StartInstances",
      "ec2:GetConsoleOutput",
      "ec2:GetConsoleScreenshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [

```



```

        "drs.amazonaws.com"
    ]
}
},
{
    "Sid" : "ConsoleFullAccess22",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
        "Null" : {
            "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
            "aws:ViaAWSService" : "true"
        }
    }
},
{
    "Sid" : "ConsoleFullAccess23",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DetachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
        "Bool" : {
            "aws:ViaAWSService" : "true"
        }
    }
},
{
    "Sid" : "ConsoleFullAccess24",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
    }
}

```

```

    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  },
  {
    "Sid" : "ConsoleFullAccess25",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ],
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess26",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateSecurityGroup",
          "CreateVolume",
          "CreateSnapshot",
          "RunInstances"
        ]
      }
    }
  }
]

```

```
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  },
  {
    "Sid" : "ConsoleFullAccess27",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateLaunchTemplate"
        ]
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess28",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStacks",
      "cloudformation:ListStacks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess29",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Descrizione: questa policy fornisce l'accesso completo a tutte le API pubbliche di AWS Elastic Disaster Recovery (AWS DRS), nonché a tutte le API pubbliche di altri AWS servizi utilizzati da AWS DRS Console. Allega questa policy ai tuoi utenti o ruoli.

AWSElasticDisasterRecoveryConsoleFullAccess_v2 è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryConsoleFullAccess_v2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2023, 13:35 UTC
- Ora modificata: 19 maggio 2024, 07:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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 Elastic Disaster Recovery Conversion Server Role",
      "arn:aws:iam::*:role/service-role/
AWS Elastic Disaster Recovery Recovery Instance Role",
      "arn:aws:iam::*:role/service-role/
AWS Elastic Disaster Recovery Recovery Instance With Launch Actions Role"
    ],
    "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",
    "ssm:DescribeParameters"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ConsoleFullAccess31",
  "Effect" : "Allow",
  "Action" : [

```

```

    "ssm:SendCommand",
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
    "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
    "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
    "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
    "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
    "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
    "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
    "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
  ],
  "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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryConversionServerPolicy

Descrizione: questa policy è associata al ruolo di istanza del server AWS Elastic Disaster Recovery Conversion. Questa policy consente ai server di conversione Elastic Disaster Recovery (DRS), che sono istanze EC2 lanciate da Elastic Disaster Recovery (DRS), di comunicare con il servizio DRS. Un ruolo IAM con questa policy viene collegato (come profilo di istanza EC2) da DRS ai server di conversione DRS, che vengono avviati e terminati automaticamente da DRS, quando necessario. Non è consigliabile collegare questa policy ai propri utenti o ruoli IAM. I server di conversione DRS vengono utilizzati da Elastic Disaster Recovery quando gli utenti scelgono di ripristinare i server di origine utilizzando la console DRS, la CLI o l'API.

AWSElasticDisasterRecoveryConversionServerPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti `AWSElasticDisasterRecoveryConversionServerPolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 13:42 UTC
- Ora modificata: 27 novembre 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Descrizione: questa policy consente a AWS Elastic Disaster Recovery (DRS) di supportare la replica tra account e il failback tra account.

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryCrossAccountReplicationPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 maggio 2023, 07:16 UTC
- Ora modificata: 17 gennaio 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryEc2InstancePolicy

Descrizione: questa policy consente l'installazione e l'utilizzo del AWS Replication Agent, utilizzato da AWS Elastic Disaster Recovery (DRS) per ripristinare i server di origine eseguiti su EC2 (multiregione o Cross-AZ). Un ruolo IAM con questa policy deve essere allegato (come profilo di istanza EC2) alle istanze EC2.

AWSElasticDisasterRecoveryEc2InstancePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryEc2InstancePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 maggio 2022, 12:30 UTC
- Ora modificata: 27 novembre 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Descrizione: puoi allegare la AWSElasticDisasterRecoveryFailbackInstallationPolicy policy alle tue identità IAM. Questa policy consente di installare l'Elastic Disaster Recovery Failback Client, che viene utilizzato per eseguire il failback delle istanze di ripristino sull'infrastruttura di origine originale. Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante l'esecuzione dell'Elastic Disaster Recovery Failback Client.

AWSElasticDisasterRecoveryFailbackInstallationPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryFailbackInstallationPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2021, 11:02 UTC
- Ora modificata: 27 novembre 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryFailbackPolicy

Descrizione: questa policy consente l'utilizzo dell'Elastic Disaster Recovery Failback Client, utilizzato per il failback delle istanze di ripristino sull'infrastruttura di origine originale. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

AWSElasticDisasterRecoveryFailbackPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSElasticDisasterRecoveryFailbackPolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 10:41 UTC
- Ora modificata: 27 novembre 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

Descrizione: questa policy consente di utilizzare le autorizzazioni richieste da Amazon SSM e servizi aggiuntivi per eseguire azioni post-lancio in AWS Elastic Disaster Recovery (AWS DRS). Allega questa policy ai tuoi ruoli o utenti IAM.

AWSElasticDisasterRecoveryLaunchActionsPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryLaunchActionsPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 settembre 2023, 07:38 UTC
- Ora modificata: 19 maggio 2024, 07:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
```

```

        "ssm:DescribeParameters"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "drs.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "LaunchActionsPolicy2",
    "Effect" : "Allow",
    "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
    ],
    "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
    ],
    "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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Descrizione: questa policy consente a AWS Elastic Disaster Recovery (DRS) di supportare la replica di rete.

AWSElasticDisasterRecoveryNetworkReplicationPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryNetworkReplicationPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 giugno 2023, 12:36 UTC
- Ora modificata: 02 gennaio 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryReadOnlyAccess

Descrizione: puoi allegare la AWSElasticDisasterRecoveryReadOnlyAccess policy alle tue identità IAM. Questa policy fornisce le autorizzazioni a tutte le API pubbliche di sola lettura di Elastic Disaster Recovery (DRS), nonché ad alcune API di sola lettura di altri AWS servizi necessarie per utilizzare appieno la console DRS in sola lettura. Collega questa policy ai tuoi utenti o ruoli IAM.

AWSElasticDisasterRecoveryReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2021, 10:50 UTC
- Ora modificata: 27 novembre 2023, 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Descrizione: questa policy è associata al ruolo di istanza dell'istanza di ripristino di Elastic Disaster Recovery. Questa policy consente all'istanza di ripristino Elastic Disaster Recovery (DRS), che sono istanze EC2 lanciate da Elastic Disaster Recovery, di comunicare con il servizio DRS e di effettuare il failback sull'infrastruttura di origine originale. Un ruolo IAM con questa policy è associato (come profilo di istanza EC2) da Elastic Disaster Recovery alle istanze di ripristino DRS. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

AWSElasticDisasterRecoveryRecoveryInstancePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryRecoveryInstancePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 10:20 UTC
- Ora modificata: 27 novembre 2023, 13:11 UTC

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

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

Descrizione: questa policy è associata al ruolo di istanza del server Elastic Disaster Recovery Replication. Questa policy consente ai server di replica Elastic Disaster Recovery (DRS), che sono istanze EC2 lanciate da Elastic Disaster Recovery (DRS), di comunicare con il servizio DRS e di creare istantanee EBS nel tuo Account AWS. Un ruolo IAM con questa policy è associato (come profilo di istanza EC2) da Elastic Disaster Recovery ai server di replica DRS, che vengono avviati e terminati automaticamente da DRS, in base alle esigenze. I server di replica DRS vengono utilizzati per facilitare la replica dei dati dai server esterni a AWS, come parte del processo di ripristino gestito da DRS. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

AWSElasticDisasterRecoveryReplicationServerPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryReplicationServerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 13:34 UTC
- Ora modificata: 27 novembre 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryServiceRolePolicy

Descrizione: questa policy consente a Elastic Disaster Recovery di gestire AWS le risorse per tuo conto.

AWSElasticDisasterRecoveryServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 novembre 2021, 10:56 UTC
- Ora modificata: 17 gennaio 2024, 13:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

Descrizione: questa policy consente l'accesso in sola lettura alle risorse AWS Elastic Disaster Recovery (DRS) come server di origine e job. Consente inoltre di creare un'istantanea convertita e di condividerla con un account specifico.

AWSElasticDisasterRecoveryStagingAccountPolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryStagingAccountPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio

- Ora di creazione: 26 maggio 2022, 09:49 UTC
- Ora modificata: 27 novembre 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Descrizione: questa policy viene utilizzata da AWS Elastic Disaster Recovery (DRS) per ripristinare i server di origine in un account di destinazione separato e per consentire il failback. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElasticDisasterRecoveryStagingAccountPolicy_v2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 gennaio 2023, 12:11 UTC
- Ora modificata: 27 novembre 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

Descrizione: Policy Service Linked Role per AWS Elastic Load Balancing Control Plane - Classic

AWSElasticLoadBalancingClassicServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 settembre 2017, 22:36 UTC
- Ora modificata: 07 ottobre 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElasticLoadBalancingServiceRolePolicy

Descrizione: policy Service Linked Role per AWS Elastic Load Balancing Control Plane

AWSElasticLoadBalancingServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 settembre 2017, 22:19 UTC
- Ora modificata: 26 agosto 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaConvertFullAccess

Descrizione: fornisce l'accesso completo a AWS Elemental MediaConvert tramite l'SDK AWS Management Console and.

AWSElementalMediaConvertFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaConvertFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 giugno 2018, 19:25 UTC
- Ora modificata: 10 giugno 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWS ElementalMediaConvertReadOnly

Descrizione: fornisce l'accesso in sola lettura a AWS Elemental MediaConvert tramite l'SDK AWS Management Console and.

AWS ElementalMediaConvertReadOnly è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSElementalMediaConvertReadOnly` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 giugno 2018, 19:25 UTC
- Ora modificata: 10 giugno 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaLiveFullAccess

Descrizione: fornisce l'accesso completo alle risorse AWS elementali MediaLive

AWSElementalMediaLiveFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaLiveFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 luglio 2020, 17:07 UTC
- Ora modificata: 08 luglio 2020, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Effect" : "Allow",
"Action" : "medialive:*",
"Resource" : "*"
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaLiveReadOnly

Descrizione: fornisce l'accesso in sola lettura alle AWS risorse elementali MediaLive

AWSElementalMediaLiveReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaLiveReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 luglio 2020, 16:38 UTC
- Ora modificata: 08 luglio 2020, 16:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaPackageFullAccess

Descrizione: fornisce l'accesso completo alle risorse AWS elementali MediaPackage

AWSElementalMediaPackageFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaPackageFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 dicembre 2017, 23:39 UTC
- Ora modificata: 29 dicembre 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaPackageReadOnly

Descrizione: fornisce l'accesso in sola lettura alle AWS risorse elementali MediaPackage

AWSElementalMediaPackageReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaPackageReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 30 dicembre 2017, 00:04 UTC
- Ora modificata: 30 dicembre 2017, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaPackageV2FullAccess

Descrizione: fornisce l'accesso completo alle risorse AWS Elemental MediaPackage V2.

AWSElementalMediaPackageV2FullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSElementalMediaPackageV2FullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 luglio 2023, 20:29 UTC
- Ora modificata: 25 luglio 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaPackageV2ReadOnly

Descrizione: fornisce accesso in sola lettura alle risorse AWS MediaPackage Elemental V2.

AWSElementalMediaPackageV2ReadOnly è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaPackageV2ReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 luglio 2023, 20:31 UTC
- Ora modificata: 25 luglio 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaStoreFullAccess

Descrizione: fornisce accesso completo in lettura e scrittura a tutte le MediaStore API

AWSElementalMediaStoreFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaStoreFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 marzo 2018, 23:15 UTC
- Ora modificata: 5 marzo 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Action" : [
    "mediastore:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "aws:SecureTransport" : "true"
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaStoreReadOnly

Descrizione: fornisce autorizzazioni di sola lettura per le API MediaStore

AWSElementalMediaStoreReadOnly è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaStoreReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 8 marzo 2018, 19:48 UTC
- Ora modificata: 08 marzo 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaTailorFullAccess

Descrizione: fornisce l'accesso completo alle risorse AWS elementali MediaTailor

AWSElementalMediaTailorFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaTailorFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 novembre 2021, 00:04 UTC
- Ora modificata: 23 novembre 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSElementalMediaTailorReadOnly

Descrizione: fornisce l'accesso in sola lettura alle AWS risorse elementali MediaTailor

AWSElementalMediaTailorReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSElementalMediaTailorReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 novembre 2021, 00:05 UTC
- Ora modificata: 23 novembre 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSEnhancedClassicNetworkingMangementPolicy

Descrizione: Politica per abilitare la funzionalità classica avanzata di gestione della rete.

AWSEnhancedClassicNetworkingMangementPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 settembre 2017, 17:29 UTC
- Ora modificata: 20 settembre 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSEntityResolutionConsoleFullAccess

Descrizione: fornisce l'accesso completo da console a AWS Entity Resolution e ai servizi correlati.

AWSEntityResolutionConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSEntityResolutionConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 agosto 2023, 17:54 UTC
- Ora modificata: 16 ottobre 2023, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSEntityResolutionConsoleReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Entity Resolution tramite. AWS Management Console

AWSEntityResolutionConsoleReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSEntityResolutionConsoleReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 agosto 2023, 18:18 UTC
- Ora modificata: 17 agosto 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFaultInjectionSimulatorEC2Access

Descrizione: questa policy concede l'autorizzazione al servizio Fault Injection Simulator in EC2 e ad altri servizi necessari per eseguire azioni FIS.

AWSFaultInjectionSimulatorEC2Access [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSFaultInjectionSimulatorEC2Access ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:39 UTC
- Ora modificata: 27 novembre 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFaultInjectionSimulatorECSAccess

Descrizione: questa policy concede l'autorizzazione al servizio Fault Injection Simulator in ECS e ad altri servizi necessari per eseguire azioni FIS.

AWSFaultInjectionSimulatorECSAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSFaultInjectionSimulatorECSAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:37 UTC
- Ora modificata: 25 gennaio 2024, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"br/>  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFaultInjectionSimulatorEKSAccess

Descrizione: questa politica concede l'autorizzazione al servizio Fault Injection Simulator in EKS e ad altri servizi necessari per eseguire le azioni FIS.

AWSFaultInjectionSimulatorEKSAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSFaultInjectionSimulatorEKSAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:34 UTC
- Ora modificata: 13 novembre 2023, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFaultInjectionSimulatorNetworkAccess

Descrizione: questa policy concede al servizio Fault Injection Simulator l'autorizzazione per le reti EC2 e altri servizi necessari per eseguire azioni FIS.

AWSFaultInjectionSimulatorNetworkAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSFaultInjectionSimulatorNetworkAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:32 UTC
- Ora modificata: 25 gennaio 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFaultInjectionSimulatorRDSAccess

Descrizione: questa politica concede al servizio Fault Injection Simulator l'autorizzazione a utilizzare RDS e altri servizi necessari per eseguire azioni FIS.

AWSFaultInjectionSimulatorRDSAccess [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSFaultInjectionSimulatorRDSAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:30 UTC
- Ora modificata: 13 novembre 2023, 16:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFaultInjectionSimulatorSSMAccess

Descrizione: questa politica concede al servizio Fault Injection Simulator l'autorizzazione in SSM e altri servizi necessari per eseguire azioni FIS.

AWSFaultInjectionSimulatorSSMAccess [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSFaultInjectionSimulatorSSMAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 15:33 UTC
- Ora modificata: 02 giugno 2023, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"br/>  }br/>]br/>}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFinSpaceServiceRolePolicy

Descrizione: Politica per consentire l'accesso Servizio AWS e le risorse utilizzate o gestite da Amazon FinSpace

AWSFinSpaceServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 maggio 2023, 16:42 UTC
- Ora modificata: 01 dicembre 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFMAdminFullAccess

Descrizione: accesso completo per AWS FM Administrator

AWSFMAdminFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSFMAdminFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2018, 18:06 UTC
- Ora modificata: 20 ottobre 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"  
    ]  
  }  
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFMAdminReadOnlyAccess

Descrizione: Accesso in sola lettura per AWS FM Administrator che consente il monitoraggio delle operazioni AWS FM

AWSFMAdminReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSFMAdminReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2018, 20:07 UTC
- Ora modificata: 31 ottobre 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSFMMemberReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle azioni AWS WAF per gli account membri di AWS Firewall Manager

AWSFMMemberReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSFMMemberReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2018, 21:05 UTC
- Ora modificata: 09 maggio 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSForWordPressPluginPolicy

Descrizione: politica gestita AWS per il plugin For Wordpress

AWSForWordPressPluginPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSForWordPressPluginPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 ottobre 2019, 00:27 UTC
- Ora modificata: 20 gennaio 2020, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGitSyncServiceRolePolicy

Descrizione: Policy che consente a AWS Code Connections di sincronizzare i contenuti dal tuo repository git

AWSGitSyncServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 novembre 2023, 17:05 UTC
- Ora modificata: 26 aprile 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
}  
  }  
  ]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGlobalAcceleratorSLRPolicy

Descrizione: Politica di concessione delle autorizzazioni a AWS Global Accelerator per gestire le interfacce di rete elastiche e i gruppi di sicurezza EC2.

AWSGlobalAcceleratorSLRPolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 aprile 2019, 19:39 UTC
- Ora modificata: 12 settembre 2023, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGlueConsoleFullAccess

Descrizione: Fornisce l'accesso completo a AWS Glue tramite AWS Management Console

AWSGlueConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSGlueConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 agosto 2017, 13:37 UTC
- Ora modificata: 14 luglio 2023, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGlueConsoleSageMakerNotebookFullAccess

Descrizione: Fornisce l'accesso completo a AWS Glue tramite AWS Management Console e l'accesso alle istanze del notebook sagemaker.

AWSGlueConsoleSageMakerNotebookFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSGlueConsoleSageMakerNotebookFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 ottobre 2018, 17:52 UTC
- Ora modificata: 15 luglio 2021, 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AwsGlueDataBrewFullAccessPolicy

Descrizione: Fornisce l'accesso completo a AWS Glue DataBrew tramite AWS Management Console. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3, KMS, Glue).

AwsGlueDataBrewFullAccessPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AwsGlueDataBrewFullAccessPolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 novembre 2020, 16:51 UTC
- Ora modificata: 04 febbraio 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGlueDataBrewServiceRole

Descrizione: questa politica concede il permesso a glue di eseguire azioni sul catalogo dati Glue dell'utente, questa politica fornisce anche l'autorizzazione alle azioni ec2 per consentire a glue di creare ENI per connettersi alle risorse nel VPC, inoltre consentire a glue di accedere ai dati registrati in lakeformation e il permesso di accedere al cloudwatch dell'utente

AWSGlueDataBrewServiceRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AWSGlueDataBrewServiceRole` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 04 dicembre 2020, 21:26 UTC
- Ora modificata: 20 marzo 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGlueSchemaRegistryFullAccess

Descrizione: Fornisce l'accesso completo al servizio AWS Glue Schema Registry

AWSGlueSchemaRegistryFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSGlueSchemaRegistryFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2020, 00:19 UTC
- Ora modificata: 20 novembre 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGlueSchemaRegistryReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al servizio AWS Glue Schema Registry

AWSGlueSchemaRegistryReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSGlueSchemaRegistryReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2020, 00:20 UTC
- Ora modificata: 20 novembre 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGlueServiceNotebookRole

Descrizione: ruolo del servizio Policy for AWS Glue che consente al cliente di gestire il server notebook

AWSGlueServiceNotebookRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSGlueServiceNotebookRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 13:37 UTC
- Ora modificata: 09 ottobre 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
}
]
```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGlueServiceRole

Descrizione: ruolo del servizio Policy for AWS Glue che consente l'accesso a servizi correlati tra cui EC2, S3 e Cloudwatch Logs

AWSGlueServiceRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSGlueServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 13:37 UTC
- Ora modificata: 11 settembre 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  ]
}
]
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AwsGlueSessionUserRestrictedNotebookPolicy

Descrizione: fornisce autorizzazioni che consentono agli utenti di creare e utilizzare solo le sessioni di notebook associate all'utente. Questa politica include anche le autorizzazioni per consentire esplicitamente agli utenti di passare un ruolo di sessione Glue limitato.

AwsGlueSessionUserRestrictedNotebookPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AwsGlueSessionUserRestrictedNotebookPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 aprile 2022, 15:24 UTC
- Ora modificata: 22 novembre 2023, 01:32 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

Descrizione: Fornisce l'accesso completo a tutte le risorse AWS Glue ad eccezione delle sessioni. Permette agli utenti di creare e utilizzare solo le sessioni notebook associate all'utente. Questa politica include anche altre autorizzazioni necessarie a AWS Glue per gestire le risorse Glue in altri AWS servizi.

AwsGlueSessionUserRestrictedNotebookServiceRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AwsGlueSessionUserRestrictedNotebookServiceRole` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 aprile 2022, 15:27 UTC
- Ora modificata: 18 aprile 2022, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    ]
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AwsGlueSessionUserRestrictedPolicy

Descrizione: fornisce autorizzazioni che consentono agli utenti di creare e utilizzare solo le sessioni interattive associate all'utente. Questa politica include anche le autorizzazioni per consentire esplicitamente agli utenti di passare un ruolo di sessione Glue limitato.

AwsGlueSessionUserRestrictedPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AwsGlueSessionUserRestrictedPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 aprile 2022, 21:31 UTC
- Ora modificata: 29 aprile 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:user}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",

```

```
        "glue:CancelStatement",
        "glue:StopSession",
        "glue>DeleteSession",
        "glue:GetSession"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/owner" : "${aws:userid}"
        }
    }
},
{
    "Sid" : "AllowListSessions",
    "Effect" : "Allow",
    "Action" : [
        "glue:ListSessions"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "DenyTagActions",
    "Effect" : "Deny",
    "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:TagKeys" : [
                "owner"
            ]
        }
    }
},
},
```

```
{
  "Sid" : "AllowPassRoleActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AwsGlueSessionUserRestrictedServiceRole

Descrizione: Fornisce l'accesso completo a tutte le risorse AWS Glue ad eccezione delle sessioni. Permette agli utenti di creare e utilizzare solo le sessioni interattive associate all'utente. Questa politica include anche altre autorizzazioni necessarie a AWS Glue per gestire le risorse Glue in altri AWS servizi.

AwsGlueSessionUserRestrictedServiceRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AwsGlueSessionUserRestrictedServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 aprile 2022, 21:30 UTC
- Ora modificata: 29 aprile 2024, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    }
  ]
}
```



```
]
},
{
  "Sid" : "AllowCompletionActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:StartCompletion",
    "glue:GetCompletion"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:completion/*"
  ]
},
{
  "Sid" : "AllowSessionActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/owner" : "${aws:user}"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
},
{
  "Sid" : "AllowStatementActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:RunStatement",
    "glue:GetStatement",
    "glue:ListStatements",
    "glue:CancelStatement",
    "glue:StopSession",
    "glue>DeleteSession",
    "glue:GetSession"
```

```
    ],
    "Resource" : [
        "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/owner" : "${aws:userid}"
        }
    }
},
{
    "Sid" : "AllowListSessionsAction",
    "Effect" : "Allow",
    "Action" : [
        "glue:ListSessions"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "DenyTagActions",
    "Effect" : "Deny",
    "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:TagKeys" : [
                "owner"
            ]
        }
    }
},
{
    "Sid" : "AllowS3BucketActions",
    "Effect" : "Allow",
    "Action" : [
```

```
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/**",
        "arn:aws:s3:::*/**aws-glue-*/**"
      ]
    },
    {
      "Sid" : "AllowS3ObjectCrawlerActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Sid" : "AllowLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*/aws-glue/*"
      ]
    },
    {
      "Sid" : "AllowTagsActions",
      "Effect" : "Allow",
```

```
"Action" : [
  "ec2:CreateTags",
  "ec2:DeleteTags"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "aws-glue-service-resource"
    ]
  }
},
"Resource" : [
  "arn:aws:ec2:*:*:network-interface/*",
  "arn:aws:ec2:*:*:security-group/*",
  "arn:aws:ec2:*:*:instance/*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGrafanaAccountAdministrator

Descrizione: fornisce l'accesso all'interno di Amazon Grafana per creare e gestire aree di lavoro per l'intera organizzazione.

AWSGrafanaAccountAdministrator è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSGrafanaAccountAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 febbraio 2021, 00:20 UTC
- Ora modificata: 15 febbraio 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGrafanaConsoleReadOnlyAccess

Descrizione: accesso alle operazioni di sola lettura in Amazon Grafana.

AWSGrafanaConsoleReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSGrafanaConsoleReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 febbraio 2021, 00:10 UTC
- Ora modificata: 15 febbraio 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGrafanaWorkspacePermissionManagement

Descrizione: offre solo la possibilità di aggiornare le autorizzazioni utente e di gruppo per le aree di lavoro AWS Grafana.

AWSGrafanaWorkspacePermissionManagement [è una politica gestita AWS](#) .

Utilizzo di questa politica

Puoi collegarti `AWSGrafanaWorkspacePermissionManagement` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 febbraio 2021, 00:15 UTC
- Ora modificata: 15 marzo 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGrafanaWorkspacePermissionManagementV2

Descrizione: offre la possibilità di aggiornare le autorizzazioni di utenti e gruppi di IAM Identity Center (iDC) per le aree di lavoro Amazon Managed Grafana.

AWSGrafanaWorkspacePermissionManagementV2 [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSGrafanaWorkspacePermissionManagementV2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 gennaio 2024, 18:39 UTC

- Ora modificata: 5 gennaio 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGreengrassFullAccess

Descrizione: questa politica offre pieno accesso alle azioni di configurazione, gestione e implementazione di AWS Greengrass

AWSGreengrassFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSGreengrassFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 maggio 2017, 00:47 UTC
- Ora modificata: 03 maggio 2017, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGreengrassReadOnlyAccess

Descrizione: questa policy consente l'accesso in sola lettura alle azioni di configurazione, gestione e implementazione di AWS Greengrass

AWSGreengrassReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSGreengrassReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 ottobre 2018, 16:01 UTC
- Ora modificata: 30 ottobre 2018, 16:01 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGreengrassResourceAccessRolePolicy

Descrizione: ruolo del servizio Policy for AWS Greengrass che consente l'accesso a servizi correlati, tra cui i thing shadow AWS Lambda e AWS IoT.

AWSGreengrassResourceAccessRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti `AWSGreengrassResourceAccessRolePolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 febbraio 2017, 21:17 UTC
- Ora modificata: 14 novembre 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSGroundStationAgentInstancePolicy

Descrizione: fornisce all'istanza Dataflow Endpoint le autorizzazioni per utilizzare l'agente Ground Station AWS

AWSGroundStationAgentInstancePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSGroundStationAgentInstancePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 marzo 2023, 15:23 UTC
- Ora modificata: 29 marzo 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSHealth_EventProcessorServiceRolePolicy

Descrizione: consente a AWS Health di abilitare la funzionalità Health Event Processor.

AWSHealth_EventProcessorServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 gennaio 2023, 19:24 UTC
- Ora modificata: 13 gennaio 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSHealthFullAccess

Descrizione: consente l'accesso completo alle API e alle notifiche AWS Health e alla Personal Health Dashboard

AWSHealthFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSHealthFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 dicembre 2016, 12:30 UTC
- Ora modificata: 16 novembre 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSHealthImagingFullAccess

Descrizione: Fornisce l'accesso completo al servizio AWS Health Imaging.

AWSHealthImagingFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSHealthImagingFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 luglio 2023, 23:39 UTC
- Ora modificata: 25 luglio 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSHealthImagingReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura al servizio AWS Health Imaging.

AWSHealthImagingReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSHealthImagingReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 luglio 2023, 23:40 UTC
- Ora modificata: 01 agosto 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIAMIdentityCenterAllowListForIdentityContext

Descrizione: fornisce l'elenco delle azioni consentite per i ruoli assunti con il contesto di identità IAM Identity Center. AWS Security Token Service (AWS STS) associa automaticamente questa policy ai ruoli presunti. Il contesto di identità viene passato come `ProvidedContext`.

AWSIAMIdentityCenterAllowListForIdentityContext è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIAMIdentityCenterAllowListForIdentityContext ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 novembre 2023, 15:21 UTC
- Ora modificata: 16 maggio 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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",
"elasticmapreduce:AddJobFlowSteps",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:CancelSteps",
"elasticmapreduce:DescribeStep",
"elasticmapreduce:ListSteps",
"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",
    "q:StartConversation",
    "q:SendMessage",
    "q:ListConversations",
    "q:GetConversation",
    "q:StartTroubleshootingAnalysis",
    "q:GetTroubleshootingResults",
    "q:StartTroubleshootingResolutionExplanation",
    "q:UpdateTroubleshootingCommandResult",
    "qapps:CreateQApp",
    "qapps:PredictProblemStatementFromConversation",
    "qapps:PredictQAppFromProblemStatement",
    "qapps:CopyQApp",
    "qapps:GetQApp",
    "qapps:ListQApps",
    "qapps:UpdateQApp",
    "qapps>DeleteQApp",
    "qapps:AssociateQAppWithUser",
    "qapps:DisassociateQAppFromUser",
    "qapps:ImportDocumentToQApp",
    "qapps:ImportDocumentToQAppSession",
    "qapps>CreateLibraryItem",
    "qapps:GetLibraryItem",
    "qapps:UpdateLibraryItem",
    "qapps>CreateLibraryItemReview",
    "qapps:ListLibraryItems",
    "qapps>CreateSubscriptionToken",
    "qapps:StartQAppSession",
    "qapps:StopQAppSession",
    "qbusiness:Chat",
    "qbusiness:ChatSync",
    "qbusiness:ListConversations",
    "qbusiness:ListMessages",
    "qbusiness>DeleteConversation",
    "qbusiness:PutFeedback",
    "sts:SetContext"
  ],
  "Resource" : "*"
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIdentitySyncFullAccess

Descrizione: concede l'accesso completo al servizio Identity Sync

AWSIdentitySyncFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIdentitySyncFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2022, 23:29 UTC
- Ora modificata: 23 marzo 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIdentitySyncReadOnlyAccess

Descrizione: accesso in sola lettura al servizio Identity Sync

AWSIdentitySyncReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIdentitySyncReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2022, 23:29 UTC
- Ora modificata: 23 marzo 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSImageBuilderFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni di AWS Image Builder e l'accesso con ambito di risorse ai servizi correlati. AWS

AWSImageBuilderFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSImageBuilderFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 dicembre 2019, 18:25 UTC
- Ora modificata: 13 aprile 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSImageBuilderReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a tutte le azioni di AWS Image Builder.

AWSImageBuilderReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSIAMReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 dicembre 2019, 22:29 UTC
- Ora modificata: 19 dicembre 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSImportExportFullAccess

Descrizione: fornisce l'accesso in lettura e scrittura ai lavori creati con Account AWS.

AWSImportExportFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSImportExportFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSImportExportReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ai lavori creati con Account AWS.

AWSImportExportReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSImportExportReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

Descrizione: concede a Incident Manager le autorizzazioni per chiamare altri AWS servizi come parte della gestione di un incidente.

AWSIncidentManagerIncidentAccessServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIncidentManagerIncidentAccessServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2023, 00:01 UTC
- Ora modificata: 20 febbraio 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "*"br/>  }br/>]br/>}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIncidentManagerResolverAccess

Descrizione: questa politica concede le autorizzazioni per avviare, visualizzare e aggiornare gli incidenti con accesso completo agli eventi cronologici personalizzati e agli elementi correlati.

Assegna questa politica agli utenti che creeranno e risolveranno gli incidenti.

AWSIncidentManagerResolverAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIncidentManagerResolverAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 10 maggio 2021, 06:12 UTC
- Ora modificata: 10 maggio 2021, 06:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIncidentManagerServiceRolePolicy

Descrizione: questa politica concede a Incident Manager l'autorizzazione a gestire i record degli incidenti e le risorse correlate per conto dell'utente.

AWSIncidentManagerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 maggio 2021, 03:34 UTC
- Ora modificata: 05 dicembre 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoT1ClickFullAccess

Descrizione: Fornisce l'accesso completo a AWS IoT 1-Click.

AWSIoT1ClickFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoT1ClickFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2018, 22:10 UTC
- Ora modificata: 11 maggio 2018, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Action" : [
    "iot1click:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoT1ClickReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura a AWS IoT 1-Click.

AWSIoT1ClickReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoT1ClickReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2018, 21:49 UTC
- Ora modificata: 11 maggio 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTAnalyticsFullAccess

Descrizione: Fornisce l'accesso completo a IoT Analytics.

AWSIoTAnalyticsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTAnalyticsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 giugno 2018, 23:02 UTC
- Ora modificata: 18 giugno 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTAnalyticsReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a IoT Analytics.

AWSIoTAnalyticsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTAnalyticsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 giugno 2018, 21:37 UTC
- Ora modificata: 18 giugno 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTConfigAccess

Descrizione: questa policy offre l'accesso completo alle azioni di configurazione AWS IoT

AWSIoTConfigAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTConfigAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 ottobre 2015, 21:52 UTC
- Ora modificata: 27 settembre 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTConfigReadOnlyAccess

Descrizione: questa policy consente l'accesso in sola lettura alle azioni di configurazione AWS IoT

AWSIoTConfigReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTConfigReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 ottobre 2015, 21:52 UTC
- Ora modificata: 27 settembre 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDataAccess

Descrizione: questa policy offre l'accesso completo alle azioni di messaggistica AWS IoT

AWSIoTDataAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTDataAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 ottobre 2015, 21:51 UTC
- Ora modificata: 23 giugno 2021, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Descrizione: fornisce accesso in scrittura ai gruppi di oggetti IoT e accesso in lettura ai certificati IoT per l'esecuzione dell'azione di mitigazione ADD_THINGS_TO_THING_GROUP

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction è [una](#) politica gestita.AWS

Utilizzo di questa politica

Puoi collegarti AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:55 UTC
- Ora modificata: 07 agosto 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceDefenderAudit

Descrizione: Fornisce accesso in lettura per l'IoT e le risorse correlate

AWSIoTDeviceDefenderAudit è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTDeviceDefenderAudit ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 luglio 2018, 21:17 UTC
- Ora modificata: 25 novembre 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
      ]
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Descrizione: fornisce l'accesso per abilitare la registrazione IoT per l'esecuzione dell'azione di mitigazione `ENABLE_IOT_LOGGING`

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` è [AWS una](#) politica gestita.

Utilizzo di questa politica

Puoi collegarti `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:04 UTC
- Ora modificata: 07 agosto 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Descrizione: fornisce l'accesso alla pubblicazione dei messaggi sull'argomento SNS per l'esecuzione dell'azione di mitigazione PUBLISH_FINDING_TO_SNS

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction è [AWS una](#) politica gestita.

Utilizzo di questa politica

Puoi collegarti AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:04 UTC
- Ora modificata: 07 agosto 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    "sns:Publish"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Descrizione: fornisce l'accesso in scrittura alle policy IoT per l'esecuzione dell'azione di mitigazione REPLACE_DEFAULT_POLICY_VERSION

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction è [una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:04 UTC
- Ora modificata: 07 agosto 2019, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Descrizione: fornisce l'accesso in scrittura ai certificati CA IoT per l'esecuzione dell'azione di mitigazione UPDATE_CA_CERTIFICATE

AWSIoTDeviceDefenderUpdateCACertMitigationAction è [una](#) politica gestita AWS

Utilizzo di questa politica

Puoi collegarti `AWSIoTDeviceDefenderUpdateCACertMitigationAction` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:05 UTC
- Ora modificata: 07 agosto 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Descrizione: fornisce l'accesso in scrittura ai certificati IoT per l'esecuzione dell'azione di mitigazione UPDATE_DEVICE_CERTIFICATE

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction è [una](#) politica gestita AWS

Utilizzo di questa politica

Puoi collegarti AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:06 UTC
- Ora modificata: 07 agosto 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

Descrizione: consente a AWS IoT Device Tester di eseguire la suite di qualificazione FreerTOS consentendo l'accesso a servizi tra cui IoT, S3 e IAM

AWSIoTDeviceTesterForFreeRTOSFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSIoTDeviceTesterForFreeRTOSFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 febbraio 2020, 20:33 UTC

- Ora modificata: 10 agosto 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTDeviceTesterForGreengrassFullAccess

Descrizione: consente a AWS IoT Device Tester di eseguire la suite di qualificazione AWS Greengrass consentendo l'accesso ai servizi correlati tra cui Lambda, IoT, API Gateway, IAM

AWSIoTDeviceTesterForGreengrassFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSIoTDeviceTesterForGreengrassFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 febbraio 2020, 21:21 UTC
- Ora modificata: 25 giugno 2020, 17:01 UTC

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

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}

```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTEventsFullAccess

Descrizione: Fornisce l'accesso completo a IoT Events.

AWSIoTEventsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTEventsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 10 gennaio 2019, 22:51 UTC
- Ora modificata: 10 gennaio 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTEventsReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a IoT Events.

AWSIoTEventsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTEventsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 10 gennaio 2019, 22:50 UTC
- Ora modificata: 23 settembre 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoT FleetHubFederationAccess

Descrizione: Accesso federativo per le applicazioni IoT Fleet Hub

AWSIoT FleetHubFederationAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoT FleetHubFederationAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 15 dicembre 2020, 08:08 UTC
- Ora modificata: 04 aprile 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoT FleetHubFederationAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  }
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoT Fleetwise Service Role Policy

Descrizione: concede le autorizzazioni alle AWS risorse e ai metadati utilizzati o gestiti da AWSIoT Fleetwise per le funzionalità ausiliarie

AWSIoT Fleetwise Service Role Policy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 settembre 2022, 23:27 UTC
- Ora modificata: 21 settembre 2022, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoT Fleetwise Service Role Policy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTFullAccess

Descrizione: questa policy offre l'accesso completo alla configurazione AWS IoT e alle azioni di messaggistica

AWSIoTFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSIoTFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 ottobre 2015, 15:19 UTC
- Ora modificata: 19 maggio 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTLogging

Descrizione: consente la creazione di gruppi Amazon CloudWatch Log e di log di streaming verso i gruppi

AWSIoTLogging è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTLogging ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 8 ottobre 2015, 15:17 UTC
- Ora modificata: 8 ottobre 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Action" : [
  "logs:CreateLogGroup",
  "logs:CreateLogStream",
  "logs:PutLogEvents",
  "logs:PutMetricFilter",
  "logs:PutRetentionPolicy",
  "logs:GetLogEvents",
  "logs>DeleteLogStream"
],
"Resource" : [
  "*"
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTOTAUpdate

Descrizione: consente l'accesso per creare AWS IoT Job e descrivere il lavoro di AWS code signer

AWSIoTOTAUpdate è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTOTAUpdate ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 dicembre 2017, 20:36 UTC
- Ora modificata: 20 dicembre 2017, 20:36 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTRoboRunnerFullAccess

Descrizione: questa politica concede autorizzazioni che consentono l'accesso completo all' AWS IoT. RoboRunner

AWSIoTRoboRunnerFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSIotRoboRunnerFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 03:54 UTC
- Ora modificata: 23 febbraio 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTRoboRunnerReadOnly

Descrizione: questa politica concede autorizzazioni che consentono l'accesso in sola lettura all'Iot. AWS RoboRunner

AWSIoTRoboRunnerReadOnly è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSIoTRoboRunnerReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 03:43 UTC
- Ora modificata: 16 novembre 2022, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTRoboRunnerServiceRolePolicy

Descrizione: consente RoboRunner all' AWS IoT di gestire AWS le risorse associate per conto del cliente.

AWSIoTRoboRunnerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 febbraio 2023, 16:56 UTC
- Ora modificata: 21 febbraio 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTRuleActions

Descrizione: consente l'accesso a tutti i AWS servizi supportati in AWS IoT Rule Actions

AWSIoTRuleActions è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTRuleActions ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 8 ottobre 2015, 15:14 UTC
- Ora modificata: 16 gennaio 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTSiteWiseConsoleFullAccess

Descrizione: Fornisce l'accesso completo alla gestione dell' AWS IoT SiteWise utilizzando AWS Management Console. Nota che questa policy consente anche l'accesso alla creazione e all'elenco degli archivi dati utilizzati con AWS IoT SiteWise (ad esempio AWS IoT Analytics), l'accesso all'elenco e alla visualizzazione delle risorse AWS IoT Greengrass, l'elenco e la modifica dei segreti di Secrets AWS Manager, il recupero delle thing shadow AWS IoT, l'elenco delle risorse con tag specifici e la creazione e l'utilizzo di un ruolo collegato ai servizi per IoT. AWS SiteWise

AWSIoTSiteWiseConsoleFullAccess è una [AWS politica](#) gestita.

Utilizzo di questa politica

Puoi collegarti AWSIoTSiteWiseConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 31 maggio 2019, 21:37 UTC
- Ora modificata: 31 maggio 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTSiteWiseFullAccess

Descrizione: Fornisce l'accesso completo all'IoT SiteWise.

AWSIoTSiteWiseFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTSiteWiseFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 dicembre 2018, 20:53 UTC

- Ora modificata: 04 dicembre 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTSiteWiseMonitorPortalAccess

Descrizione: questa policy concede le autorizzazioni per accedere agli SiteWise asset AWS IoT e ai dati degli asset, creare risorse AWS IoT SiteWise Monitor ed elencare gli utenti AWS SSO.

AWSIoTSiteWiseMonitorPortalAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTSiteWiseMonitorPortalAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 maggio 2020, 20:01 UTC
- Ora modificata: 19 maggio 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

Descrizione: questo ruolo concede le autorizzazioni di SiteWise monitoraggio AWS IoT per accedere alle risorse e alle proprietà degli SiteWise asset AWS IoT e creare progetti AWS IoT Sitewise, dashboard e politiche di accesso tramite portali IoT. AWS SiteWise

AWSIoTSiteWiseMonitorServiceRolePolicy [è una policy gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 novembre 2019, 00:59 UTC
- Ora modificata: 13 dicembre 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTSiteWiseReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura all'IoT SiteWise.

AWSIoTSiteWiseReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTSiteWiseReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 dicembre 2018, 20:55 UTC

- Ora modificata: 16 settembre 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTThingsRegistration

Descrizione: questa politica consente agli utenti di registrare elementi in blocco utilizzando l'API AWS IoT StartThingRegistrationTask

AWSIoTThingsRegistration è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTThingsRegistration ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2017, 20:21 UTC
- Ora modificata: 5 ottobre 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTtwinMakerServiceRolePolicy

Descrizione: consente TwinMaker all' AWS IoT di chiamare altri AWS servizi e di sincronizzare le relative risorse per conto dell'utente.

AWSIoTtwinMakerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 novembre 2023, 18:59 UTC
- Ora modificata: 13 novembre 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"  
        ]  
    }  
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTWirelessDataAccess

Descrizione: consente l'accesso ai dati di identità associati ai dispositivi AWS IoT Wireless.

AWSIoTWirelessDataAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTWirelessDataAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:31 UTC
- Ora modificata: 15 dicembre 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTWirelessFullAccess

Descrizione: consente all'identità associata l'accesso completo a tutte le operazioni AWS IoT Wireless.

AWSIoTWirelessFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTWirelessFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:27 UTC
- Ora modificata: 15 dicembre 2020, 15:27 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTWirelessFullPublishAccess

Descrizione: fornisce l'accesso completo a IoT Wireless per la pubblicazione su IoT Rules Engine per tuo conto.

AWSIoTWirelessFullPublishAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSIoTWirelessFullPublishAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:29 UTC
- Ora modificata: 15 dicembre 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTWirelessGatewayCertManager

Descrizione: consente l'accesso all'identità associata per creare, elencare e descrivere i certificati IoT

AWSIoTWirelessGatewayCertManager è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTWirelessGatewayCertManager ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:30 UTC
- Ora modificata: 15 dicembre 2020, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTWirelessLogging

Descrizione: consente all'identità associata di creare gruppi Amazon CloudWatch Logs e trasmettere log ai gruppi.

AWSIoTWirelessLogging è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTWirelessLogging ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:32 UTC
- Ora modificata: 15 dicembre 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIoTWirelessReadOnlyAccess

Descrizione: consente all'identità associata di accedere in sola lettura al wireless AWS IoT.

AWSIoTWirelessReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIoTWirelessReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:28 UTC
- Ora modificata: 15 dicembre 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIPAMServiceRolePolicy

Descrizione: consente a VPC IP Address Manager di accedere alle risorse VPC e di integrarsi con AWS Organizations per tuo conto.

AWSIPAMServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 novembre 2021, 19:08 UTC
- Ora modificata: 08 novembre 2023, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIQContractServiceRolePolicy

Descrizione: Utilizzato da AWS IQ per eseguire le richieste di pagamento per conto di un cliente

AWSIQContractServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 22 agosto 2019, 19:28 UTC
- Ora modificata: 22 agosto 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIQFullAccess

Descrizione: Fornisce accesso completo a AWS IQ

AWSIQFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSIQFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 aprile 2019, 23:13 UTC
- Ora modificata: 25 settembre 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSIQPermissionServiceRolePolicy

Descrizione: consente a AWS IQ di gestire il ruolo assunto dagli esperti di IQ AWS .

AWSIQPermissionServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 22 agosto 2019, 19:36 UTC
- Ora modificata: 22 agosto 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Descrizione: consente l'accesso ai AWS servizi e alle risorse necessari per gli archivi di chiavi personalizzati AWS KMS

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 novembre 2018, 20:10 UTC
- Ora modificata: 10 novembre 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Descrizione: consente a AWS KMS di sincronizzare le proprietà condivise delle chiavi multiregionali.

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 giugno 2021, 15:37 UTC
- Ora modificata: 16 giugno 2021, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSKeyManagementServicePowerUser

Descrizione: fornisce l'accesso al AWS Key Management Service (KMS).

AWSKeyManagementServicePowerUser è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSKeyManagementServicePowerUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 07 marzo 2017, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLakeFormationCrossAccountManager

Descrizione: fornisce l'accesso da più account alle risorse Glue tramite Lake Formation. Garantisce inoltre l'accesso in lettura ad altri servizi richiesti, come le organizzazioni e il gestore dell'accesso alle risorse

AWSLakeFormationCrossAccountManager è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSLakeFormationCrossAccountManager ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 04 agosto 2020, 20:59 UTC
- Ora modificata: 22 marzo 2024, 18:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram>DeleteResourceShare",
        "ram:AssociateResourceShare",
```



```

        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ram:ResourceShareName" : [
                "LakeFormation*"
            ]
        }
    }
},
{
    "Sid" : "AllowManageResourceSharePermissions",
    "Effect" : "Allow",
    "Action" : [
        "ram:AssociateResourceSharePermission"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "ram:PermissionArn" : [
                "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
            ]
        }
    }
},
{
    "Sid" : "AllowXAcctManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "glue:PutResourcePolicy",
        "glue>DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowOrganizationsPermissions",
    "Effect" : "Allow",
    "Action" : [

```

```
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLakeFormationDataAdmin

Descrizione: Concede l'accesso amministrativo a AWS Lake Formation e ai servizi correlati, come AWS Glue, per la gestione dei data lake

AWSLakeFormationDataAdmin è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSLakeFormationDataAdmin ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 agosto 2019, 17:33 UTC
- Ora modificata: 22 marzo 2024, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "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:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue>DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",

```

```
    "iam:GetRolePolicy"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSLakeFormationDataAdminDeny",
  "Effect" : "Deny",
  "Action" : [
    "lakeformation:PutDataLakeSettings"
  ],
  "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambda_FullAccess

Descrizione: concede l'accesso completo al servizio AWS Lambda, alle funzionalità della console AWS Lambda e ad altri servizi correlati. AWS

AWSLambda_FullAccess [è una politica gestita AWS](#) .

Utilizzo di questa politica

Puoi collegarti AWSLambda_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2020, 21:14 UTC
- Ora modificata: 17 novembre 2020, 21:14 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ],
  "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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambda_ReadOnlyAccess

Descrizione: concede l'accesso in sola lettura al servizio AWS Lambda, alle funzionalità della console AWS Lambda e ad altri servizi correlati. AWS

AWSLambda_ReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSLambda_ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2020, 21:10 UTC
- Ora modificata: 27 luglio 2023, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaBasicExecutionRole

Descrizione: fornisce autorizzazioni di scrittura per i CloudWatch registri.

AWSLambdaBasicExecutionRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSLambdaBasicExecutionRole` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 9 aprile 2015, 15:03 UTC
- Ora modificata: 9 aprile 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaDynamoDBExecutionRole

Descrizione: Fornisce accesso in lista e lettura ai flussi DynamoDB e autorizzazioni di scrittura nei log. CloudWatch

AWSLambdaDynamoDBExecutionRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSLambdaDynamoDBExecutionRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 9 aprile 2015, 15:09 UTC
- Ora modificata: 9 aprile 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Action" : [
  "dynamodb:DescribeStream",
  "dynamodb:GetRecords",
  "dynamodb:GetShardIterator",
  "dynamodb:ListStreams",
  "logs:CreateLogGroup",
  "logs:CreateLogStream",
  "logs:PutLogEvents"
],
"Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaENIManagementAccess

Descrizione: fornisce le autorizzazioni minime per una funzione Lambda per gestire gli ENI (creazione, descrizione, eliminazione) utilizzati da una funzione Lambda abilitata per VPC.

AWSLambdaENIManagementAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSLambdaENIManagementAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 dicembre 2016, 00:37 UTC
- Ora modificata: 01 ottobre 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaExecute

Descrizione: fornisce Put, Get Access a S3 e accesso completo ai CloudWatch log.

AWSLambdaExecute è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSLambdaExecute ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaFullAccess

Descrizione: questa politica si trova su un percorso obsoleto. Consulta la documentazione come guida: <https://docs.aws.amazon.com/lambda/latest/dg/.html>. access-control-identity-based Fornisce accesso completo a Lambda, S3, DynamoDB, Metrics and Logs. CloudWatch

AWSLambdaFullAccess è [una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSLambdaFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 27 novembre 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaInvocation-DynamoDB

Descrizione: Fornisce accesso in lettura a DynamoDB Streams.

AWSLambdaInvocation-DynamoDB [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSLambdaInvocation-DynamoDB ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaKinesisExecutionRole

Descrizione: fornisce l'accesso in modalità elenco e lettura agli stream Kinesis e autorizzazioni di scrittura nei log. CloudWatch

AWSLambdaKinesisExecutionRole è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSLambdaKinesisExecutionRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 9 aprile 2015, 15:14 UTC
- Ora modificata: 19 novembre 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaMSKExecutionRole

Descrizione: fornisce le autorizzazioni necessarie per accedere al cluster MSK all'interno di un VPC, gestire ENI (creazione, descrizione, eliminazione) nel VPC e scrivere le autorizzazioni nei registri. CloudWatch

AWSLambdaMSKExecutionRole è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSLambdaMSKExecutionRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 agosto 2020, 17:35 UTC
- Ora modificata: 02 agosto 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaReplicator

Descrizione: concede a Lambda Replicator le autorizzazioni necessarie per replicare le funzioni tra le regioni

AWSLambdaReplicator [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 maggio 2017, 17:53 UTC
- Ora modificata: 08 dicembre 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaRole

Descrizione: politica predefinita per il ruolo del servizio AWS Lambda.

AWSLambdaRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSLambdaRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaSQSQueueExecutionRole

Descrizione: fornisce l'accesso agli attributi di ricezione, eliminazione di messaggi e lettura alle code SQS e autorizzazioni di scrittura per i log. CloudWatch

AWSLambdaSQSQueueExecutionRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSLambdaSQSQueueExecutionRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 giugno 2018, 21:50 UTC
- Ora modificata: 14 giugno 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLambdaVPCAccessExecutionRole

Descrizione: fornisce autorizzazioni minime per l'esecuzione di una funzione Lambda durante l'accesso a una risorsa all'interno di un VPC: creazione, descrizione, eliminazione di interfacce di rete e autorizzazioni di scrittura nei registri. CloudWatch

AWSLambdaVPCAccessExecutionRole è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AWSLambdaVPCAccessExecutionRole` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 febbraio 2016, 23:15 UTC
- Ora modificata: 5 gennaio 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLicenseManagerConsumptionPolicy

Descrizione: fornisce le autorizzazioni per consentire l'accesso alle azioni dell'API AWS License Manager necessarie per utilizzare le licenze per le quali l'utente dispone dei diritti.

AWSLicenseManagerConsumptionPolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSLicenseManagerConsumptionPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 agosto 2021, 23:18 UTC
- Ora modificata: 11 agosto 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Descrizione: consente al servizio AWS License Manager Linux Subscriptions di gestire le risorse per conto dell'utente.

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi

- Ora di creazione: 20 dicembre 2022, 18:54 UTC
- Ora modificata: 20 dicembre 2022, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLicenseManagerMasterAccountRolePolicy

Descrizione: politica del ruolo dell'account principale del servizio AWS License Manager

AWSLicenseManagerMasterAccountRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 novembre 2018, 19:03 UTC
- Ora modificata: 31 maggio 2022, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
          ]
        }
      }
    }
  ]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLicenseManagerMemberAccountRolePolicy

Descrizione: politica relativa al ruolo degli account dei membri del servizio AWS License Manager

AWSLicenseManagerMemberAccountRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 novembre 2018, 19:04 UTC
- Ora modificata: 15 novembre 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
            "*"
        ]
    }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLicenseManagerServiceRolePolicy

Descrizione: politica dei ruoli predefiniti del servizio AWS License Manager

AWSLicenseManagerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 novembre 2018, 19:02 UTC
- Ora modificata: 30 luglio 2021, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
    ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Descrizione: consente al servizio AWS License Manager User Subscriptions di gestire le risorse per conto dell'utente.

AWSLicenseManagerUserSubscriptionsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 luglio 2022, 01:17 UTC
- Ora modificata: 21 novembre 2022, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSM2ServicePolicy

Descrizione: consente a AWS M2 di gestire AWS le risorse per tuo conto.

AWSM2ServicePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 07 giugno 2022, 20:26 UTC
- Ora modificata: 07 giugno 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSManagedServices_ContactsServiceRolePolicy

Descrizione: consente AWS a Managed Services di leggere i valori dei tag sulle AWS risorse

AWSManagedServices_ContactsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 marzo 2023, 17:07 UTC
- Ora modificata: 23 marzo 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Descrizione: AWS Managed Services: policy per gestire l'infrastruttura dei controlli investigativi

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 dicembre 2022, 23:11 UTC
- Ora modificata: 19 dicembre 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSManagedServices_EventsServiceRolePolicy

Descrizione: policy di AWS Managed Services per abilitare la funzionalità del processore di eventi AMS.

AWSManagedServices_EventsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 07 febbraio 2023, 18:41 UTC
- Ora modificata: 07 febbraio 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"   
}  
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSManagedServicesDeploymentToolkitPolicy

Descrizione: consente AWS a Managed Services di gestire il toolkit di distribuzione per conto dell'utente.

AWSManagedServicesDeploymentToolkitPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 09 giugno 2022, 18:33 UTC
- Ora modificata: 04 aprile 2024, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AMSCDKToolkitS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
```

```

        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
    ],
    "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
},
{
    "Sid" : "AMSCDKToolkitCloudFormationPermissions",
    "Effect" : "Allow",
    "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateTerminationProtection"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
},
{
    "Sid" : "AMSCDKToolkitECRPermissions",
    "Effect" : "Allow",
    "Action" : [
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:CreateRepository",
        "ecr>DeleteLifecyclePolicy",
        "ecr>DeleteRepository",
        "ecr>DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",

```

```
    "ecr:PutImageScanningConfiguration",
    "ecr:PutImageTagMutability",
    "ecr:PutLifecyclePolicy",
    "ecr:SetRepositoryPolicy",
    "ecr:TagResource",
    "ecr:UntagResource"
  ],
  "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceAmiIngestion

Descrizione: Consente di Marketplace AWS copiare le tue Amazon Machine Images (AMI) per elencarle su Marketplace AWS

AWSMarketplaceAmiIngestion è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceAmiIngestion ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 settembre 2020, 20:55 UTC
- Ora modificata: 25 settembre 2020, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceDeploymentServiceRolePolicy

Descrizione: consente di Marketplace AWS creare e gestire i parametri di distribuzione del venditore per i prodotti a cui ti abboni Marketplace AWS.

AWSMarketplaceDeploymentServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 15 novembre 2023, 23:34 UTC
- Ora modificata: 15 novembre 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
        }
    }
}
]

```

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceFullAccess

Descrizione: offre la possibilità di sottoscrivere e annullare l'iscrizione al Marketplace AWS software, consente agli utenti di gestire le istanze del software Marketplace dalla pagina «Il tuo software» di Marketplace e fornisce l'accesso amministrativo a EC2.

AWSMarketplaceFullAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 febbraio 2015, 17:21 UTC
- Ora modificata: 04 marzo 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
      ]
    }
  }
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceGetEntitlements

Descrizione: fornisce l'accesso in lettura ai Marketplace AWS diritti

AWSMarketplaceGetEntitlements è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceGetEntitlements ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 marzo 2017, 19:37 UTC
- Ora modificata: 5 aprile 2024, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AWSMarketplaceGetEntitlements",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:GetEntitlements"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceImageBuildFullAccess

Descrizione: fornisce l'accesso completo alla funzione Marketplace AWS Private Image Build. Oltre a creare immagini private, fornisce anche le autorizzazioni per aggiungere tag alle immagini, avviare e terminare le istanze ec2.

AWSMarketplaceImageBuildFullAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceImageBuildFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 31 luglio 2018, 23:29 UTC
- Ora modificata: 04 marzo 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Marketplace AWS per la gestione delle licenze.

AWSMarketplaceLicenseManagementServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 03 dicembre 2020, 08:33 UTC
- Ora modificata: 03 dicembre 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceManageSubscriptions

Descrizione: offre la possibilità di sottoscrivere e annullare l'iscrizione al software Marketplace AWS

AWSMarketplaceManageSubscriptions è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceManageSubscriptions ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 19 gennaio 2023, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceMeteringFullAccess

Descrizione: fornisce l'accesso completo a Marketplace AWS Metering.

AWSMarketplaceMeteringFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceMeteringFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 marzo 2016, 22:39 UTC
- Ora modificata: 17 marzo 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceMeteringRegisterUsage

Descrizione: fornisce le autorizzazioni per registrare una risorsa e tenere traccia dell'utilizzo tramite il servizio di Marketplace AWS misurazione.

AWSMarketplaceMeteringRegisterUsage è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceMeteringRegisterUsage ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 novembre 2019, 01:17 UTC
- Ora modificata: 21 novembre 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceProcurementSystemAdminFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni amministrative per un'integrazione di Marketplace AWS eProcurement.

AWSMarketplaceProcurementSystemAdminFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceProcurementSystemAdminFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 giugno 2019, 13:07 UTC
- Ora modificata: 25 giugno 2019, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

Descrizione: consente l'accesso ai Marketplace AWS servizi per la gestione degli ordini di acquisto.

AWSMarketplacePurchaseOrdersServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 27 ottobre 2021, 15:12 UTC
- Ora modificata: 27 ottobre 2021, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceRead-only

Descrizione: offre la possibilità di rivedere Marketplace AWS gli abbonamenti

AWSMarketplaceRead-only è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceRead-only ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 19 gennaio 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Marketplace AWS For Resale Authorization.

AWSMarketplaceResaleAuthorizationServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 marzo 2024, 18:47 UTC
- Ora modificata: 5 marzo 2024, 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceSellerFullAccess

Descrizione: Fornisce l'accesso completo a tutte le operazioni del venditore relative a servizi Marketplace AWS e ad altri AWS servizi come la gestione degli AML.

AWSMarketplaceSellerFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceSellerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2019, 20:40 UTC
- Ora modificata: 15 marzo 2024, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceSellerProductsFullAccess

Descrizione: fornisce ai venditori l'accesso completo alla pagina Marketplace AWS dei prodotti di gestione e ad altri AWS servizi come la gestione AMI.

AWSMarketplaceSellerProductsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceSellerProductsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2019, 21:06 UTC
- Ora modificata: 18 luglio 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMarketplaceSellerProductsReadOnly

Descrizione: fornisci ai venditori l'accesso in sola lettura alla pagina dei prodotti di Marketplace AWS gestione.

AWSMarketplaceSellerProductsReadOnly [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSMarketplaceSellerProductsReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2019, 21:40 UTC
- Ora modificata: 19 novembre 2022, 00:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMediaConnectServicePolicy

Descrizione: la politica predefinita che consente l'accesso Servizi AWS e le risorse utilizzate o gestite da MediaConnect.

AWSMediaConnectServicePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 3 aprile 2023 22:11 UTC
- Ora modificata: 03 aprile 2023, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMediaTailorServiceRolePolicy

Descrizione: Abilita l'accesso alle AWS risorse utilizzate o gestite da MediaTailor

AWSMediaTailorServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 settembre 2021, 22:27 UTC
- Ora modificata: 17 settembre 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubDiscoveryAccess

Descrizione: la politica AWSMigrationHubService consente di chiamare per AWSApplicationDiscoveryService conto del cliente.

AWSMigrationHubDiscoveryAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubDiscoveryAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 13:30 UTC
- Ora modificata: 6 agosto 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubDMSAccess

Descrizione: Politica per l'assunzione del ruolo del Database Migration Service nell'account del cliente per chiamare Migration Hub

AWSMigrationHubDMSAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubDMSAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 14:00 UTC
- Ora modificata: 07 ottobre 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubFullAccess

Descrizione: policy gestita per fornire al cliente l'accesso al servizio Migration Hub

AWSMigrationHubFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 agosto 2017, 14:02 UTC
- Ora modificata: 19 giugno 2019, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubOrchestratorConsoleFullAccess

Descrizione: Fornisce un accesso limitato a AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service e AWS Secrets Manager. Questa politica garantisce inoltre l'accesso completo al servizio AWS Migration Hub Orchestrator.

AWSMigrationHubOrchestratorConsoleFullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubOrchestratorConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 20 aprile 2022, 02:26 UTC
- Ora modificata: 05 dicembre 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

Descrizione: questa policy deve essere allegata per le istanze migrate da SAP e MGN per consentire al nostro servizio di orchestrare le istanze scaricando script da S3 e recuperare valori segreti all'interno dell'istanza EC2.

AWSMigrationHubOrchestratorInstanceRolePolicy è una [politica](#) gestita AWS

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubOrchestratorInstanceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2022, 02:43 UTC
- Ora modificata: 20 aprile 2022, 02:43 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubOrchestratorPlugin

Descrizione: fornisce un accesso limitato alle azioni relative ad Amazon Simple Storage Service, AWS Secrets Manager e Plugin per AWS Migration Hub Orchestrator.

AWSMigrationHubOrchestratorPlugin [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubOrchestratorPlugin ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2022, 02:25 UTC
- Ora modificata: 20 aprile 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubOrchestratorServiceRolePolicy

Descrizione: Fornisce le autorizzazioni necessarie a Migration Hub Orchestrator per migrare e modernizzare i carichi di lavoro locali

AWSMigrationHubOrchestratorServiceRolePolicy è [una politica gestita](#).AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 aprile 2022, 02:24 UTC
- Ora modificata: 4 marzo 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubRefactorSpaces- EnvironmentsWithoutBridgesFullAccess

Descrizione: concede l'accesso completo a AWS Migration Hub Refactor Spaces e ad altri servizi AWS correlati ad eccezione dei gruppi di sicurezza AWS Transit Gateway e EC2 non richiesti quando si utilizzano ambienti senza un bridge di rete. Questa politica esclude anche le autorizzazioni richieste per AWS Lambda e AWS Resource Access Manager in quanto possono essere delimitate in base ai tag.

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 aprile 2023, 20:09 UTC
- Ora modificata: 11 aprile 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```

        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
    ],
    "Resource" : "*"
},
{
    "Sid" : "VpcEndpointServiceConfigurationCreate",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
    ],
    "Resource" : "*"
},
{
    "Sid" : "EC2TagsDelete",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteTags"
    ],
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
    }
},
{
    "Sid" : "VpcEndpointServiceConfigurationDelete",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
    }
},
{
    "Sid" : "ELBLoadBalancerCreate",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:AddTags",

```

```

        "elasticloadbalancing:CreateLoadBalancer"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
    }
},
{
    "Sid" : "ELBDescribe",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ELBModify",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing>DeleteListener",
        "elasticloadbalancing>DeleteTargetGroup"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/refactor-spaces:route-id" : [
                "*"
            ]
        }
    }
},
{
    "Sid" : "ELBLoadBalancerDelete",
    "Effect" : "Allow",

```

```

    "Action" : "elasticloadbalancing:DeleteLoadBalancer",
    "Resource" : "arn*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
  },
  {
    "Sid" : "ELBListenerCreate",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateListener"
    ],
    "Resource" : [
      "arn*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
      "arn*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  },
  {
    "Sid" : "ELBListenerDelete",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DeleteListener",
    "Resource" : "arn*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
  },
  {
    "Sid" : "ELBTargetGroupModify",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DeleteTargetGroup",
      "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : "arn*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
  },
  {
    "Sid" : "ELBTargetGroupCreate",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateTargetGroup"
    ],
    "Resource" : "arn*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",

```

```

    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [

```

```
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudformationStackCreate",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudformationStackTag",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:TagResource"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/*"
},
{
  "Sid" : "CreateRefactorSpacesSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
    }
  }
},
{
  "Sid" : "CreateELBSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
    }
  }
}
]
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Descrizione: utilizzo nel ruolo di servizio IAM passato al documento AWSRefactorSpaces di automazione SSM CreateResources per concedere le autorizzazioni necessarie per eseguire l'automazione. La policy concede l'accesso in lettura/scrittura ai tag EC2 per tenere traccia dei progressi dell'automazione. Quando il bridge di rete dell'ambiente Refactor Spaces è abilitato, l'automazione aggiunge anche il gruppo di sicurezza dell'ambiente all'istanza EC2 per consentire il traffico proveniente da altri servizi Refactor Spaces presenti nell'ambiente. La policy consente inoltre l'accesso ai parametri SSM delle azioni successive al lancio dell'Application Migration Service.

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubRefactorSpaces-SSMAutomationPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 agosto 2023, 15:08 UTC
- Ora modificata: 10 agosto 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-
*"
    }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubRefactorSpacesFullAccess

Descrizione: concede l'accesso completo a AWS MigrationHub Refactor Spaces, alle funzionalità della console di AWS MigrationHub Refactor Spaces e ad altri AWS servizi correlati, ad eccezione delle autorizzazioni richieste per Lambda e AWS Resource Access AWS Manager in quanto possono essere delimitate in base ai tag.

AWSMigrationHubRefactorSpacesFullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AWSMigrationHubRefactorSpacesFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 07:12 UTC
- Ora modificata: 11 aprile 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```

        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
    ],
    "Resource" : "*"
},
{
    "Sid" : "RequestTagTransitGatewayCreate",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
    ],
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
    }
},
{
    "Sid" : "ResourceTagTransitGatewayCreate",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
    ],
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
    }
},
{
    "Sid" : "VpcEndpointServiceConfigurationCreate",
    "Effect" : "Allow",
    "Action" : [

```

```

    "ec2:CreateVpcEndpointServiceConfiguration"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2NetworkingModify",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteTransitGateway",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:DeleteSecurityGroup",
    "ec2:DeleteTransitGatewayVpcAttachment",
    "ec2:CreateRoute",
    "ec2:DeleteRoute",
    "ec2:DeleteTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:environment-id" : "false"
    }
  }
},
{
  "Sid" : "VpcEndpointServiceConfigurationDelete",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Sid" : "ELBLoadBalancerCreate",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateLoadBalancer"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",

```

```

    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:application-id" : "false"
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing>CreateLoadBalancerListeners",
        "elasticloadbalancing>CreateListener",
        "elasticloadbalancing>DeleteListener",
        "elasticloadbalancing>DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing>DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
  ],

```

```

{
  "Sid" : "ELBListenerCreate",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateListener"
  ],
  "Resource" : [
    "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
    "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
},
{
  "Sid" : "ELBListenerDelete",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DeleteListener",
  "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
},
{
  "Sid" : "ELBTargetGroupModify",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DeleteTargetGroup",
    "elasticloadbalancing:RegisterTargets"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
},
{
  "Sid" : "ELBTargetGroupCreate",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateTargetGroup"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
}

```

```
    }
  },
  {
    "Sid" : "APIGatewayModify",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "apigateway:DELETE",
      "apigateway:PATCH",
      "apigateway:POST",
      "apigateway:PUT",
      "apigateway:UpdateRestApiPolicy"
    ],
    "Resource" : [
      "arn:aws:apigateway:*::/restapis",
      "arn:aws:apigateway:*::/restapis/*",
      "arn:aws:apigateway:*::/vpclinks",
      "arn:aws:apigateway:*::/vpclinks/*",
      "arn:aws:apigateway:*::/tags",
      "arn:aws:apigateway:*::/tags/*"
    ],
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Sid" : "APIGatewayVpcLinksGet",
    "Effect" : "Allow",
    "Action" : "apigateway:GET",
    "Resource" : [
      "arn:aws:apigateway:*::/vpclinks",
      "arn:aws:apigateway:*::/vpclinks/*"
    ]
  },
  {
    "Sid" : "OrganizationDescribe",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeOrganization"
    ],
    "Resource" : "*"
  },
}
```

```
{
  "Sid" : "CloudformationStackCreate",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudformationStackTag",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:TagResource"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/*"
},
{
  "Sid" : "CreateRefactorSpacesSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
    }
  }
},
{
  "Sid" : "CreateELBSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
    }
  }
}
]
```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate da AWS Migration Hub Refactor Spaces.

AWSMigrationHubRefactorSpacesServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 29 novembre 2021, 06:50 UTC
- Ora modificata: 20 luglio 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubSMSAccess

Descrizione: Politica per l'assunzione del ruolo del servizio di migrazione dei server nell'account del cliente per chiamare Migration Hub

AWSMigrationHubSMSAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSMigrationHubSMSAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 13:57 UTC
- Ora modificata: 07 ottobre 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubStrategyCollector

Descrizione: concede le autorizzazioni per consentire la comunicazione con il servizio AWS Migration Hub Strategy Recommendations, l'accesso in lettura/scrittura ai bucket S3 relativi al servizio, l'accesso ad Amazon API Gateway su cui caricare log e metriche, l'accesso a Secrets AWS Manager per recuperare le credenziali e AWS tutti i servizi correlati.

AWSMigrationHubStrategyCollector [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubStrategyCollector ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 ottobre 2021, 20:15 UTC
- Ora modificata: 01 aprile 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```



```
    }
  },
  {
    "Sid" : "MHSRAllowS3ListBucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "arn:aws:s3:::*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "MHSRAllowMetricsAndLogs",
    "Effect" : "Allow",
    "Action" : [
      "application-transformation:PutMetricData",
      "application-transformation:PutLogData",
      "application-transformation:StartPortingCompatibilityAssessment",
      "application-transformation:GetPortingCompatibilityAssessment",
      "application-transformation:StartPortingRecommendationAssessment",
      "application-transformation:GetPortingRecommendationAssessment"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "MHSRAllowExecuteAPI",
    "Effect" : "Allow",
    "Action" : [
      "execute-api:Invoke",
      "execute-api:ManageConnections"
    ],
    "Resource" : [
      "arn:aws:execute-api:*:*:*/*prod/*/*put-log-data",
      "arn:aws:execute-api:*:*:*/*prod/*/*put-metric-data"
    ]
  },
  {
    "Sid" : "MHSRAllowCollectorAPI",
    "Effect" : "Allow",
    "Action" : [
```

```

        "migrationhub-strategy:RegisterCollector",
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration",
        "migrationhub-strategy:PutLogData",
        "migrationhub-strategy:PutMetricData"
    ],
    "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
  },
  {
    "Sid" : "MHSRAllowSecretsManager",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubStrategyConsoleFullAccess

Descrizione: concede l'accesso completo al servizio AWS Migration Hub Strategy Recommendations e l'accesso ai AWS servizi correlati tramite AWS Management Console

AWSMigrationHubStrategyConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMigrationHubStrategyConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 ottobre 2021, 20:13 UTC
- Ora modificata: 09 novembre 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMigrationHubStrategyServiceRolePolicy

Descrizione: Abilita l'accesso alle AWS risorse utilizzate o gestite dal servizio AWS Migration Hub Strategy Recommendations.

AWSMigrationHubStrategyServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 ottobre 2021, 20:02 UTC
- Ora modificata: 19 ottobre 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMobileHub_FullAccess

Descrizione: questa politica può essere allegata a qualsiasi utente, ruolo o gruppo, al fine di concedere agli utenti l'autorizzazione a creare, eliminare e modificare progetti (e AWS le relative risorse associate) in AWS Mobile Hub. Ciò include anche le autorizzazioni per generare e scaricare codice sorgente di app mobili di esempio per ogni progetto Mobile Hub.

AWSMobileHub_FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMobileHub_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 gennaio 2016, 19:56 UTC
- Ora modificata: 19 dicembre 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```



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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMobileHub_ReadOnly

Descrizione: questa politica può essere allegata a qualsiasi utente, ruolo o gruppo, al fine di concedere agli utenti l'autorizzazione a elencare e visualizzare i progetti in AWS Mobile Hub. Ciò include anche le autorizzazioni per generare e scaricare codice sorgente di app mobili di esempio per ogni progetto Mobile Hub. Non consente all'utente di modificare alcuna configurazione per alcun progetto Mobile Hub.

AWSMobileHub_ReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSMobileHub_ReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 gennaio 2016, 19:55 UTC
- Ora modificata: 23 luglio 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSMSKReplicatorExecutionRole

Descrizione: concede le autorizzazioni ad Amazon MSK Replicator per replicare i dati tra cluster MSK.

AWSMSKReplicatorExecutionRole è [una](#) politica gestita AWS.

Utilizzo di questa politica

Puoi collegarti AWSMSKReplicatorExecutionRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 06 dicembre 2023, 00:07 UTC
- Ora modificata: 25 marzo 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:WriteDataIdempotently"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
    }
  ]
}
```

```
]
},
{
  "Sid" : "TopicPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kafka-cluster:DescribeTopic",
    "kafka-cluster:CreateTopic",
    "kafka-cluster:AlterTopic",
    "kafka-cluster:WriteData",
    "kafka-cluster:ReadData",
    "kafka-cluster:DescribeTopicDynamicConfiguration",
    "kafka-cluster:AlterTopicDynamicConfiguration",
    "kafka-cluster:AlterCluster"
  ],
  "Resource" : [
    "arn:aws:kafka:*:*:topic/*/*"
  ]
},
{
  "Sid" : "GroupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kafka-cluster:AlterGroup",
    "kafka-cluster:DescribeGroup"
  ],
  "Resource" : [
    "arn:aws:kafka:*:*:group/*/*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSNetworkFirewallServiceRolePolicy

Descrizione: consente AWSNetworkFirewall di creare e gestire le risorse necessarie per i firewall.

AWSNetworkFirewallServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 novembre 2020, 17:17 UTC
- Ora modificata: 30 marzo 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSNetworkManagerCloudWANServiceRolePolicy

Descrizione: consente NetworkManager di accedere alle risorse associate alla rete principale

AWSNetworkManagerCloudWANServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 luglio 2022, 12:17 UTC
- Ora modificata: 12 luglio 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSNetworkManagerFullAccess

Descrizione: fornisce l'accesso completo ad Amazon NetworkManager tramite AWS Management Console.

AWSNetworkManagerFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSNetworkManagerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 17:37 UTC
- Ora modificata: 03 dicembre 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSNetworkManagerReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon NetworkManager tramite AWS Management Console.

AWSNetworkManagerReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSNetworkManagerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 17:35 UTC
- Ora modificata: 03 dicembre 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "networkmanager:Describe*",
      "networkmanager:Get*",
      "networkmanager:List*"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSNetworkManagerServiceRolePolicy

Descrizione: consenti l'accesso NetworkManager alle risorse associate alle tue reti globali

AWSNetworkManagerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 03 dicembre 2019, 14:03 UTC
- Ora modificata: 27 luglio 2022, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"br/>  }br/>]br/>}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOpsWorks_FullAccess

Descrizione: Fornisce accesso completo a AWS OpsWorks.

AWSOpsWorks_FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSOpsWorks_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 gennaio 2021, 16:29 UTC
- Ora modificata: 22 gennaio 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOpsWorksCloudWatchLogs

Descrizione: abilita OpsWorks le istanze con l'integrazione CWLogs abilitata per spedire i log e creare i gruppi di log richiesti

AWSOpsWorksCloudWatchLogs è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSOpsWorksCloudWatchLogs ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 marzo 2017, 17:47 UTC
- Ora modificata: 30 marzo 2017, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```



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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOpsWorksCMInstanceProfileRole

Descrizione: fornisce l'accesso a S3 per le istanze lanciate da OpsWorks CM.

AWSOpsWorksCMInstanceProfileRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSOpsWorksCMInstanceProfileRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 novembre 2016, 09:48 UTC
- Ora modificata: 23 aprile 2021, 17:34 UTC

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

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"  
    }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOpsWorksCMServiceRole

Descrizione: Service Role Policy da utilizzare per la creazione di server OpsWorks CM.

AWSOpsWorksCMServiceRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSOpsWorksCMServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 novembre 2016, 09:49 UTC
- Ora modificata: 23 aprile 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOpsWorksInstanceRegistration

Descrizione: fornisce l'accesso a un'istanza Amazon EC2 per registrarsi con uno AWS OpsWorks stack.

AWSOpsWorksInstanceRegistration è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSOpsWorksInstanceRegistration ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 3 giugno 2016, 14:23 UTC
- Ora modificata: 03 giugno 2016, 14:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOpsWorksRegisterCLI_EC2

Descrizione: politica per abilitare la registrazione delle istanze EC2 tramite la CLI OpsWorks

AWSOpsWorksRegisterCLI_EC2 è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSOpsWorksRegisterCLI_EC2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 giugno 2019, 15:56 UTC
- Ora modificata: 18 giugno 2019, 15:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOpsWorksRegisterCLI_OnPremises

Descrizione: politica per abilitare la registrazione di istanze locali tramite la CLI OpsWorks

AWSOpsWorksRegisterCLI_OnPremises [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSOpsWorksRegisterCLI_OnPremises ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 18 giugno 2019, 15:33 UTC
- Ora modificata: 18 giugno 2019, 15:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOrganizationsFullAccess

Descrizione: Fornisce l'accesso completo a AWS Organizations.

AWSOrganizationsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSOrganizationsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 novembre 2018, 20:31 UTC
- Ora modificata: 6 febbraio 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOrganizationsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Organizations AWS .

AWSOrganizationsReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSOrganizationsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 novembre 2018, 20:32 UTC
- Ora modificata: 07 giugno 2024, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOrganizationsServiceTrustPolicy

Descrizione: una politica per consentire alle AWS Organizzazioni di condividere la fiducia con altri, approvata allo Servizi AWS scopo di semplificare la configurazione del cliente.

AWSOrganizationsServiceTrustPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 ottobre 2017, 23:04 UTC
- Ora modificata: 01 novembre 2017, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOutpostsAuthorizeServerPolicy

Descrizione: questa politica concede le autorizzazioni che consentono di installare un server Outpost sulla rete locale.

AWSOutpostsAuthorizeServerPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSOutpostsAuthorizeServerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 gennaio 2023, 19:23 UTC
- Ora modificata: 04 gennaio 2023, 19:23 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSOutpostsServiceRolePolicy

Descrizione: policy Service Linked Role per consentire l'accesso alle AWS risorse gestite da AWS Outposts

AWSOutpostsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 09 novembre 2020, 22:55 UTC
- Ora modificata: 09 novembre 2020, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPanoramaApplianceRolePolicy

Descrizione: consente al software AWS IoT su un'appliance AWS Panorama di caricare i log su Amazon. CloudWatch

AWSPanoramaApplianceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPanoramaApplianceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2020, 13:13 UTC
- Ora modificata: 01 dicembre 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPanoramaApplianceServiceRolePolicy

Descrizione: consente a un'appliance AWS Panorama di caricare log su Amazon CloudWatch e di ottenere oggetti dai punti di accesso Amazon S3 creati per l'uso con Panorama. AWS

AWSPanoramaApplianceServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSPanoramaApplianceServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 ottobre 2021, 12:14 UTC

- Ora modificata: 17 gennaio 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPanoramaFullAccess

Descrizione: Fornisce accesso completo a AWS Panorama

AWSPanoramaFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPanoramaFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2020, 13:12 UTC
- Ora modificata: 12 gennaio 2022, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPanoramaGreengrassGroupRolePolicy

Descrizione: consente a una funzione AWS Lambda su un dispositivo AWS Panorama di gestire le risorse in Panorama, caricare log e metriche su Amazon e gestire oggetti in CloudWatch bucket creati per l'uso con Panorama.

AWSPanoramaGreengrassGroupRolePolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSPanoramaGreengrassGroupRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2020, 13:10 UTC
- Ora modificata: 6 gennaio 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPanoramaSageMakerRolePolicy

Descrizione: consente SageMaker ad Amazon di gestire oggetti in bucket creati per l'uso con AWS Panorama.

AWSPanoramaSageMakerRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPanoramaSageMakerRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2020, 13:13 UTC
- Ora modificata: 01 dicembre 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPanoramaServiceLinkedRolePolicy

Descrizione: consente a AWS Panorama di gestire le risorse in AWS IoT, AWS Secrets Manager e AWS Panorama.

AWSPanoramaServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 ottobre 2021, 12:12 UTC
- Ora modificata: 20 ottobre 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    ]
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPanoramaServiceRolePolicy

Descrizione: consente a AWS Panorama di gestire le risorse in Amazon S3, AWS IoT, GreenGrass AWS Lambda SageMaker, Amazon e CloudWatch Amazon Logs e di trasferire i ruoli di servizio a IoT, AWS AWS GreenGrass IoT e Amazon. SageMaker

AWSPanoramaServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSPanoramaServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2020, 13:14 UTC
- Ora modificata: 01 dicembre 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:ListGroupsWith",
    "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*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPriceListServiceFullAccess

Descrizione: fornisce l'accesso completo al servizio di AWS listino prezzi.

AWSPriceListServiceFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPriceListServiceFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 novembre 2017, 00:36 UTC
- Ora modificata: 22 novembre 2017, 00:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPRivateCAAuditor

Descrizione: fornisce ai revisori l'accesso all'autorità di certificazione AWS privata

AWSPRivateCAAuditor è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPRivateCAAuditor ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:33 UTC
- Ora modificata: 14 febbraio 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAAuditor`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPrivateCAFullAccess

Descrizione: fornisce l'accesso completo all'autorità di certificazione AWS privata

AWSPRivateCAFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPRivateCAFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:20 UTC
- Ora modificata: 14 febbraio 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPriateCAPrivilegedUser

Descrizione: fornisce agli utenti del certificato l'accesso privilegiato all'autorità di certificazione AWS privata

AWSPriateCAPrivilegedUser è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPriateCAPrivilegedUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:26 UTC
- Ora modificata: 14 febbraio 2023, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriateCAPrivilegedUser`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```


Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPRivateCAReadOnly

Descrizione: fornisce l'accesso in sola lettura all'autorità di certificazione AWS privata

AWSPRivateCAReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPRivateCAReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:30 UTC
- Ora modificata: 14 febbraio 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPriateCAUser

Descrizione: fornisce agli utenti del certificato l'accesso all'autorità di certificazione AWS privata

AWSPriateCAUser è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPriateCAUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:16 UTC

- Ora modificata: 14 febbraio 2023, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPrivateMarketplaceAdminFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni amministrative per un Marketplace AWS privato.

AWSPrivateMarketplaceAdminFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPrivateMarketplaceAdminFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 16:32 UTC
- Ora modificata: 14 febbraio 2024, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPrivateMarketplaceRequests

Descrizione: fornisce l'accesso alla creazione di richieste in un Marketplace AWS privato.

AWSPrivateMarketplaceRequests è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSPrivateMarketplaceRequests ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 ottobre 2019, 21:44 UTC
- Ora modificata: 28 ottobre 2019, 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPrivateNetworksServiceRolePolicy

Descrizione: consente a AWS Private Networks Service di gestire le risorse per conto del cliente.

AWSPrivateNetworksServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 dicembre 2021, 23:17 UTC
- Ora modificata: 16 dicembre 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSProtonCodeBuildProvisioningBasicAccess

Descrizione: le autorizzazioni CodeBuild devono eseguire una build per AWS CodeBuild Proton Provisioning.

AWSProtonCodeBuildProvisioningBasicAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSProtonCodeBuildProvisioningBasicAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 novembre 2022, 21:04 UTC

- Ora modificata: 09 novembre 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

Descrizione: consente a AWS Proton di gestire l'approvvigionamento di risorse Proton utilizzando CodeBuild e altri AWS servizi per conto dell'utente.

AWSProtonCodeBuildProvisioningServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 09 novembre 2022, 21:32 UTC
- Ora modificata: 17 maggio 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]

```

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSProtonDeveloperAccess

Descrizione: fornisce l'accesso alle API AWS Proton e alla console di gestione, ma non consente l'amministrazione di modelli o ambienti Proton.

AWSProtonDeveloperAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSProtonDeveloperAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 19:02 UTC
- Ora modificata: 6 giugno 2024, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Sid" : "ProtonPermissions",
  "Effect" : "Allow",
  "Action" : [
    "codecommit:ListRepositories",
    "codepipeline:GetPipeline",
    "codepipeline:GetPipelineExecution",
    "codepipeline:GetPipelineState",
    "codepipeline:ListPipelineExecutions",
    "codepipeline:ListPipelines",
    "codestar-connections:ListConnections",
    "codestar-connections:UseConnection",
    "proton:CancelServiceInstanceDeployment",
    "proton:CancelServicePipelineDeployment",
    "proton:CreateService",
    "proton>DeleteService",
    "proton:GetAccountRoles",
    "proton:GetAccountSettings",
    "proton:GetEnvironment",
    "proton:GetEnvironmentAccountConnection",
    "proton:GetEnvironmentTemplate",
    "proton:GetEnvironmentTemplateMajorVersion",
    "proton:GetEnvironmentTemplateMinorVersion",
    "proton:GetEnvironmentTemplateVersion",
    "proton:GetRepository",
    "proton:GetRepositorySyncStatus",
    "proton:GetResourcesSummary",
    "proton:GetService",
    "proton:GetServiceInstance",
    "proton:GetServiceTemplate",
    "proton:GetServiceTemplateMajorVersion",
    "proton:GetServiceTemplateMinorVersion",
    "proton:GetServiceTemplateVersion",
    "proton:GetTemplateSyncConfig",
    "proton:GetTemplateSyncStatus",
    "proton:ListEnvironmentAccountConnections",
    "proton:ListEnvironmentOutputs",
    "proton:ListEnvironmentProvisionedResources",
    "proton:ListEnvironments",
    "proton:ListEnvironmentTemplateMajorVersions",
    "proton:ListEnvironmentTemplateMinorVersions",
    "proton:ListEnvironmentTemplates",
    "proton:ListEnvironmentTemplateVersions",
    "proton:ListRepositories",
```

```

        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CodeStarConnectionsPermissions",
    "Effect" : "Allow",
    "Action" : "codestar-connections:PassConnection",
    "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
    }
},
{
    "Sid" : "CodeConnectionsPermissions",
    "Effect" : "Allow",
    "Action" : "codeconnections:PassConnection",
    "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
    ],
    "Condition" : {
        "StringEquals" : {

```

```
        "codeconnections:PassedToService" : "proton.amazonaws.com"
    }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSProtonFullAccess

Descrizione: fornisce l'accesso completo alle API AWS Proton e alla console di gestione. Oltre a queste autorizzazioni, è necessario anche l'accesso ad Amazon S3 per registrare pacchetti di modelli dai bucket S3, nonché l'accesso ad Amazon IAM per creare e gestire i ruoli di servizio per Proton.

AWSProtonFullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSProtonFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 19:07 UTC
- Ora modificata: 6 giugno 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid" : "CreateServiceLinkedRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/AWSServiceRoleForProtonSync",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "sync.proton.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CodeStarConnectionsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:PassConnection"
    ],
    "Resource" : [
      "arn:aws:codestar-connections::*:connection/*",
      "arn:aws:codeconnections::*:connection/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "codestar-connections:PassedToService" : "proton.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CodeConnectionsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "codeconnections:PassConnection"
    ],
    "Resource" : [
      "arn:aws:codestar-connections::*:connection/*",
      "arn:aws:codeconnections::*:connection/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "codeconnections:PassedToService" : "proton.amazonaws.com"
      }
    }
  }
}

```

```
}  
  }  
    }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSProtonReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle API AWS Proton e alla console di gestione.

AWSProtonReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSProtonReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 19:09 UTC
- Ora modificata: 18 novembre 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSProtonServiceGitSyncServiceRolePolicy

Descrizione: Politica che consente a AWS Proton di sincronizzare le definizioni del servizio, dell'ambiente e dei componenti dal repository git a Proton. AWS

AWSProtonServiceGitSyncServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 4 aprile 2023, 15:55 UTC

- Ora modificata: 04 aprile 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSProtonSyncServiceRolePolicy

Descrizione: Politica che consente a AWS Proton di sincronizzare i contenuti del tuo repository git con Proton o di sincronizzare i contenuti di Proton con i tuoi repository git.

AWSProtonSyncServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 novembre 2021, 21:14 UTC
- Ora modificata: 5 maggio 2024, 01:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```

{
  "Sid" : "SyncToProton",
  "Effect" : "Allow",
  "Action" : [
    "proton:UpdateServiceTemplateVersion",
    "proton:UpdateServiceTemplate",
    "proton:UpdateEnvironmentTemplateVersion",
    "proton:UpdateEnvironmentTemplate",
    "proton:GetServiceTemplateVersion",
    "proton:GetServiceTemplate",
    "proton:GetEnvironmentTemplateVersion",
    "proton:GetEnvironmentTemplate",
    "proton>DeleteServiceTemplateVersion",
    "proton>DeleteEnvironmentTemplateVersion",
    "proton>CreateServiceTemplateVersion",
    "proton>CreateServiceTemplate",
    "proton>CreateEnvironmentTemplateVersion",
    "proton>CreateEnvironmentTemplate",
    "proton:ListEnvironmentTemplateVersions",
    "proton:ListServiceTemplateVersions",
    "proton>CreateEnvironmentTemplateMajorVersion",
    "proton>CreateServiceTemplateMajorVersion"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AccessGitRepos",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection",
    "codeconnections:UseConnection"
  ],
  "Resource" : [
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
  ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSPurchaseOrdersServiceRolePolicy

Descrizione: concede le autorizzazioni per visualizzare e modificare gli ordini di acquisto sulla console di fatturazione

AWSPurchaseOrdersServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSPurchaseOrdersServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 maggio 2020, 18:15 UTC
- Ora modificata: 17 luglio 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightAssetBundleExportPolicy

Descrizione: fornisce il set di autorizzazioni necessarie per eseguire le operazioni di esportazione di QuickSight Asset Bundle

AWSQuickSightAssetBundleExportPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSQuickSightAssetBundleExportPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 marzo 2024, 21:31 UTC
- Ora modificata: 27 marzo 2024, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:/*"
    },
    {
      "Sid" : "DashboardReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisReadAccess",
      "Effect" : "Allow",
```

```
    "Action" : [
      "quicksight:DescribeAnalysis",
      "quicksight:DescribeAnalysisPermissions"
    ],
    "Resource" : "arn:aws:quicksight:*:*:analysis/*"
  },
  {
    "Sid" : "DataSetReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "quicksight:DescribeDataSet",
      "quicksight:DescribeDataSetRefreshProperties",
      "quicksight:ListRefreshSchedules",
      "quicksight:DescribeDataSetPermissions"
    ],
    "Resource" : "arn:aws:quicksight:*:*:dataset/*"
  },
  {
    "Sid" : "DataSourceReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "quicksight:DescribeDataSource",
      "quicksight:DescribeDataSourcePermissions"
    ],
    "Resource" : "arn:aws:quicksight:*:*:datasource/*"
  },
  {
    "Sid" : "ThemeReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "quicksight:DescribeTheme",
      "quicksight:DescribeThemePermissions"
    ],
    "Resource" : "arn:aws:quicksight:*:*:theme/*"
  },
  {
    "Sid" : "VPCCConnectionReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "quicksight:DescribeVPCCConnection",
      "quicksight:ListVPCCConnections"
    ],
    "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
  },
}
```

```
{
  "Sid" : "RefreshScheduleReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeRefreshSchedule"
  ],
  "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
},
{
  "Sid" : "AssetBundleExportOperations",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeAssetBundleExportJob",
    "quicksight:ListAssetBundleExportJobs",
    "quicksight:StartAssetBundleExportJob"
  ],
  "Resource" : "arn:aws:quicksight:*:*:asset-bundle-export-job/*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightAssetBundleImportPolicy

Descrizione: fornisce il set di autorizzazioni necessarie per eseguire le operazioni di importazione di QuickSight Asset Bundle

AWSQuickSightAssetBundleImportPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSQuickSightAssetBundleImportPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 marzo 2024, 21:40 UTC
- Ora modificata: 27 marzo 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource",
        "quicksight:TagResource",
        "quicksight:UntagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDashboard",
        "quicksight>DeleteDashboard",
        "quicksight:DescribeDashboard",
        "quicksight:UpdateDashboard",
        "quicksight:UpdateDashboardPublishedVersion",
        "quicksight:DescribeDashboardPermissions",

```

```

        "quicksight:UpdateDashboardPermissions",
        "quicksight:UpdateDashboardLinks"
    ],
    "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
},
{
    "Sid" : "AnalysisWriteAccess",
    "Effect" : "Allow",
    "Action" : [
        "quicksight:CreateAnalysis",
        "quicksight:DeleteAnalysis",
        "quicksight:DescribeAnalysis",
        "quicksight:UpdateAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:UpdateAnalysisPermissions"
    ],
    "Resource" : "arn:aws:quicksight:*:*:analysis/*"
},
{
    "Sid" : "DataSetWriteAccess",
    "Effect" : "Allow",
    "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:DeleteDataSet",
        "quicksight:DescribeDataSet",
        "quicksight:PassDataSet",
        "quicksight:UpdateDataSet",
        "quicksight:DeleteDataSetRefreshProperties",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:PutDataSetRefreshProperties",
        "quicksight:UpdateDataSetPermissions",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:ListRefreshSchedules"
    ],
    "Resource" : "arn:aws:quicksight:*:*:dataset/*"
},
{
    "Sid" : "DataSourceWriteAccess",
    "Effect" : "Allow",
    "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:DescribeDataSource",
        "quicksight:DeleteDataSource",
        "quicksight:PassDataSource",

```

```

        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:DescribeDataSourcePermissions"
    ],
    "Resource" : "arn:aws:quicksight:*:*:datasource/*"
},
{
    "Sid" : "ThemeWriteAccess",
    "Effect" : "Allow",
    "Action" : [
        "quicksight:CreateTheme",
        "quicksight>DeleteTheme",
        "quicksight:DescribeTheme",
        "quicksight:UpdateTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:UpdateThemePermissions"
    ],
    "Resource" : "arn:aws:quicksight:*:*:theme/*"
},
{
    "Sid" : "RefreshScheduleWriteAccess",
    "Effect" : "Allow",
    "Action" : [
        "quicksight:CreateRefreshSchedule",
        "quicksight:DescribeRefreshSchedule",
        "quicksight>DeleteRefreshSchedule",
        "quicksight:UpdateRefreshSchedule"
    ],
    "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
},
{
    "Sid" : "VPCCConnectionWriteAccess",
    "Effect" : "Allow",
    "Action" : [
        "quicksight:ListVPCCConnections",
        "quicksight:CreateVPCCConnection",
        "quicksight:DescribeVPCCConnection",
        "quicksight>DeleteVPCCConnection",
        "quicksight:UpdateVPCCConnection"
    ],
    "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
},
{
    "Sid" : "AssetBundleImportOperations",

```



```
"Effect" : "Allow",
"Action" : [
  "quicksight:DescribeAssetBundleImportJob",
  "quicksight:ListAssetBundleImportJobs",
  "quicksight:StartAssetBundleImportJob"
],
"Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuicksightAthenaAccess

Descrizione: accesso Quicksight all'API Athena e ai bucket S3 utilizzati per i risultati delle query Athena

AWSQuicksightAthenaAccess [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSQuicksightAthenaAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 09 dicembre 2016, 02:31 UTC
- Ora modificata: 07 luglio 2021, 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
```

```
{
  "Resource" : [
    "arn:aws:s3:::aws-athena-query-results-*"
  ],
  {
    "Effect" : "Allow",
    "Action" : [
      "lakeformation:GetDataAccess"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightDescribeRDS

Descrizione: consente di QuickSight descrivere le risorse RDS

AWSQuickSightDescribeRDS è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSQuickSightDescribeRDS ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 novembre 2015, 23:24 UTC
- Ora modificata: 10 novembre 2015, 23:24 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightDescribeRedshift

Descrizione: consente di QuickSight descrivere le risorse Redshift

AWSQuickSightDescribeRedshift è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSQuickSightDescribeRedshift` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 novembre 2015, 23:25 UTC
- Ora modificata: 10 novembre 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightElasticsearchPolicy

Descrizione: Fornisce l'accesso alle risorse Amazon Elasticsearch di Amazon QuickSight

AWSQuickSightElasticsearchPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSQuickSightElasticsearchPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 09 settembre 2020, 17:27 UTC
- Ora modificata: 07 settembre 2021, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightIoTAnalyticsAccess

Descrizione: Offri l'accesso in QuickSight sola lettura ai set di dati di IoT Analytics

AWSQuickSightIoTAnalyticsAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSQuickSightIoTAnalyticsAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 17:00 UTC
- Ora modificata: 29 novembre 2017, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightListIAM

Descrizione: consente di QuickSight elencare le entità IAM

AWSQuickSightListIAM è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSQuickSightListIAM ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 novembre 2015, 23:25 UTC
- Ora modificata: 10 novembre 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuicksightOpenSearchPolicy

Descrizione: Fornisce l'accesso alle OpenSearch risorse Amazon da Amazon QuickSight

AWSQuicksightOpenSearchPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSQuicksightOpenSearchPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 07 settembre 2021, 23:26 UTC
- Ora modificata: 07 settembre 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightSageMakerPolicy

Descrizione: Fornisce l'accesso alle SageMaker risorse Amazon da Amazon QuickSight

AWSQuickSightSageMakerPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSQuickSightSageMakerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 gennaio 2020, 17:18 UTC
- Ora modificata: 30 ottobre 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSQuickSightTimestreamPolicy

Descrizione: AWS QuickSight accesso alle API AWS Timestream. I clienti possono associare questa policy al AWS QuickSight ruolo per consentire il recupero di dati e metadati.

AWSQuickSightTimestreamPolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSQuickSightTimestreamPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 30 settembre 2020, 21:47 UTC
- Ora modificata: 30 settembre 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSReachabilityAnalyzerServiceRolePolicy

Descrizione: consente a VPC Reachability Analyzer di accedere alle AWS risorse e integrarsi con AWS Organizations per tuo conto.

AWSReachabilityAnalyzerServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 novembre 2022, 17:12 UTC
- Ora modificata: 15 maggio 2024, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
```

```
"directconnect:DescribeDirectConnectGatewayAssociations",
"directconnect:DescribeDirectConnectGatewayAttachments",
"directconnect:DescribeDirectConnectGateways",
"directconnect:DescribeVirtualGateways",
"directconnect:DescribeVirtualInterfaces",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeCustomerGateways",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePrefixLists",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayConnects",
"ec2:DescribeTransitGatewayPeeringAttachments",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetManagedPrefixListEntries",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:SearchTransitGatewayRoutes",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"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" : "*"
},
{
  "Sid" : "ApigatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/vpclinks"
  ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSRefactoringToolkitFullAccess

Descrizione: questo criterio concede l'autorizzazione a utilizzare i AWS servizi con l'estensione AWS Toolkit for .NET Refactoring per Microsoft Visual Studio. È destinato a essere collegato a un profilo locale. AWS La policy consente di caricare artefatti dell'applicazione e scaricare gli artefatti risultanti da Amazon S3. Consente di creare applicazioni in un'immagine del contenitore utilizzando, archiviando AWS CodeBuild e recuperando le immagini da Amazon Elastic Container Registry (Amazon ECR). Inoltre, consente l'implementazione dell'applicazione su servizi container AWS come Amazon Elastic Container Service (Amazon ECS), la creazione opzionale di risorse VPC, la connessione opzionale all'infrastruttura esistente come Directory AWS Service e altri servizi correlati.

AWSRefactoringToolkitFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSRefactoringToolkitFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 ottobre 2022, 16:41 UTC
- Ora modificata: 25 marzo 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "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*"
    }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSRefactoringToolkitSidecarPolicy

Descrizione: questa policy è pensata per essere utilizzata da Amazon ECS Tasks creati per testare le applicazioni AWS utilizzando l'estensione AWS Toolkit for .NET Refactoring per Microsoft Visual Studio. La policy concede l'accesso per scaricare artefatti applicativi da Amazon S3, comunicare lo stato del Task tramite AWS Systems Manager e altri servizi richiesti.

AWSRefactoringToolkitSidecarPolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSRefactoringToolkitSidecarPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 ottobre 2022, 16:41 UTC
- Ora modificata: 29 ottobre 2022, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSrePostPrivateCloudWatchAccess

Descrizione: fornisce a Re:POST l'accesso privato per pubblicare CloudWatch i dati delle metriche

AWSrePostPrivateCloudWatchAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 15 novembre 2023, 16:37 UTC
- Ora modificata: 15 novembre 2023, 16:37 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSRepostSpaceSupportOperationsPolicy

Descrizione: questa politica consente al servizio re:Post Space di creare, gestire e risolvere i casi di supporto creati tramite l'applicazione Space.

AWSRepostSpaceSupportOperationsPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSRepostSpaceSupportOperationsPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 novembre 2023, 21:52 UTC
- Ora modificata: 26 novembre 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
```

```
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResilienceHubAssessmentExecutionPolicy

Descrizione: Policy per il ruolo del servizio AWS Resilience Hub che consente l'accesso ad altri AWS servizi per eseguire la valutazione.

AWSResilienceHubAssessmentExecutionPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSResilienceHubAssessmentExecutionPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2023, 12:32 UTC
- Ora modificata: 24 marzo 2024, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
```



```
"ec2:DescribeFastSnapshotRestores",
"ec2:DescribeFleets",
"ec2:DescribeHosts",
"ec2:DescribeInstances",
"ec2:DescribeNatGateways",
"ec2:DescribePlacementGroups",
"ec2:DescribeRegions",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ecr:DescribeRegistry",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeContainerInstances",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:ListContainerInstances",
"ecs:ListServices",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodegroup",
"eks:ListFargateProfiles",
"eks:ListNodegroups",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeSnapshots",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"fis:GetExperimentTemplate",
"fis:ListExperimentTemplates",
"fis:ListExperiments",
"fsx:DescribeFileSystems",
"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",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverEndpointIpAddresses",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"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/*"  
  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceAccessManagerFullAccess

Descrizione: Fornisce l'accesso completo a AWS Resource Access Manager

AWSResourceAccessManagerFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSResourceAccessManagerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 giugno 2019, 17:28 UTC
- Ora modificata: 04 giugno 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceAccessManagerReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Resource Access Manager.

AWSResourceAccessManagerReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSResourceAccessManagerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 dicembre 2019, 20:58 UTC
- Ora modificata: 09 dicembre 2019, 20:58 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceAccessManagerResourceShareParticipantAccess

Descrizione: fornisce l'accesso alle API AWS Resource Access Manager necessarie a un partecipante alla condivisione delle risorse.

AWSResourceAccessManagerResourceShareParticipantAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSResourceAccessManagerResourceShareParticipantAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 09 dicembre 2019, 20:41 UTC
- Ora modificata: 09 dicembre 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceAccessManagerServiceRolePolicy

Descrizione: Policy che include l'accesso in modalità Read-only Read-Only AWS Resource Access Manager alla struttura Organizations dei clienti. Contiene anche le autorizzazioni IAM per eliminare autonomamente il ruolo.

AWSResourceAccessManagerServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 novembre 2018, 19:28 UTC
- Ora modificata: 14 novembre 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceExplorerFullAccess

Descrizione: questa politica concede autorizzazioni amministrative per accedere alle risorse di Resource Explorer e concede autorizzazioni di sola lettura ad altri AWS servizi per supportare questo accesso.

AWSResourceExplorerFullAccess [AWS è una politica](#) gestita.

Utilizzo di questa politica

Puoi collegarti AWSResourceExplorerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 07 novembre 2022, 20:01 UTC
- Ora modificata: 14 novembre 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceExplorerOrganizationsAccess

Descrizione: questa politica concede autorizzazioni amministrative a Resource Explorer e concede autorizzazioni di sola lettura ad altri AWS servizi per supportare questo accesso. L'amministratore di AWS Organizations necessita di queste autorizzazioni per configurare e gestire la ricerca su più account nella console.

AWSResourceExplorerOrganizationsAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSResourceExplorerOrganizationsAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 novembre 2023, 17:01 UTC
- Ora modificata: 14 novembre 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "iam:ListResources",
        "iam: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"
        ]
      }
    }
  }
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceExplorerReadOnlyAccess

Descrizione: questa politica concede autorizzazioni di sola lettura per cercare e visualizzare le risorse di Resource Explorer e concede autorizzazioni di sola lettura ad altri servizi per supportare questo accesso. AWS

AWSResourceExplorerReadOnlyAccess è una [politica](#) gestita AWS.

Utilizzo di questa politica

Puoi collegarti AWSResourceExplorerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Tempo di creazione: 07 novembre 2022, 19:56 UTC
- Ora modificata: 14 novembre 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceExplorerServiceRolePolicy

Descrizione: consente a Resource Explorer di visualizzare risorse ed CloudTrail eventi per conto dell'utente per indicizzare le risorse per la ricerca.

AWSResourceExplorerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 25 ottobre 2022, 20:35 UTC
- Ora modificata: 20 dicembre 2023, 13:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSResourceGroupsReadOnlyAccess

Descrizione: questa è la politica di sola lettura per AWS Resource Groups

AWSResourceGroupsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSResourceGroupsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 marzo 2018, 10:27 UTC
- Ora modificata: 5 febbraio 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSRoboMaker_FullAccess

Descrizione: fornisce l'accesso completo AWS RoboMaker tramite AWS Management Console and SDK. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3, IAM).

AWSRoboMaker_FullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSRoboMaker_FullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 10 settembre 2020, 18:34 UTC
- Ora modificata: 16 settembre 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSRoboMakerReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura AWS RoboMaker tramite AWS Management Console and SDK

AWSRoboMakerReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSRoboMakerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 novembre 2018, 05:30 UTC
- Ora modificata: 28 agosto 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
```

```
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSRoboMakerServicePolicy

Descrizione: politica RoboMaker del servizio

AWSRoboMakerServicePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 novembre 2018, 06:30 UTC
- Ora modificata: 11 novembre 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSRoboMakerServiceRolePolicy

Descrizione: politica RoboMaker del servizio

AWSRoboMakerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSRoboMakerServiceRolePolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 novembre 2018, 05:33 UTC
- Ora modificata: 26 novembre 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSRolesAnywhereServicePolicy

Descrizione: consente a IAM Roles Anywhere di pubblicare metriche di servizio/utilizzo CloudWatch e di verificare lo stato delle autorità di certificazione private per tuo conto.

AWSRolesAnywhereServicePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 luglio 2022, 15:26 UTC
- Ora modificata: 05 luglio 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSS3OnOutpostsServiceRolePolicy

Descrizione: consenti al servizio Amazon S3 on Outposts di gestire le risorse di rete EC2 per tuo conto.

AWSS3OnOutpostsServiceRolePolicy [è una politica gestita AWS](#) .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 03 ottobre 2023, 20:32 UTC
- Ora modificata: 03 ottobre 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSavingsPlansFullAccess

Descrizione: Fornisce l'accesso completo al servizio Savings Plans

AWSSavingsPlansFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSavingsPlansFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 novembre 2019, 22:45 UTC
- Ora modificata: 6 novembre 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSavingsPlansReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura al servizio Savings Plans

AWSSavingsPlansReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSavingsPlansReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 novembre 2019, 22:45 UTC
- Ora modificata: 6 novembre 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSecurityHubFullAccess

Descrizione: Fornisce l'accesso completo all'utilizzo di AWS Security Hub.

AWSSecurityHubFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSecurityHubFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 23:54 UTC
- Ora modificata: 23 aprile 2024, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSecurityHubOrganizationsAccess

Descrizione: concede l'autorizzazione per abilitare e gestire AWS Security Hub all'interno di un'organizzazione. Include l'abilitazione del servizio in tutta l'organizzazione e la determinazione dell'account amministratore delegato per il servizio.

AWSSecurityHubOrganizationsAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSecurityHubOrganizationsAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 marzo 2021, 20:53 UTC
- Ora modificata: 16 novembre 2023, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSecurityHubReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle risorse del AWS Security Hub

AWSSecurityHubReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSecurityHubReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 01:34 UTC
- Ora modificata: 22 febbraio 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",

```

```
        "securityhub:BatchGet*",
        "securityhub:Describe*"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSecurityHubServiceRolePolicy

Descrizione: un ruolo collegato al servizio richiesto a AWS Security Hub per accedere alle tue risorse.

AWSSecurityHubServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 27 novembre 2018, 23:47 UTC
- Ora modificata: 27 novembre 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]

```

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogAdminFullAccess

Descrizione: fornisce l'accesso completo alle funzionalità di amministrazione del catalogo dei servizi

AWSServiceCatalogAdminFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSServiceCatalogAdminFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 febbraio 2018, 17:19 UTC
- Ora modificata: 13 aprile 2023, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogAdminReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle funzionalità di amministrazione di Service Catalog

AWSServiceCatalogAdminReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSServiceCatalogAdminReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 ottobre 2019, 18:53 UTC
- Ora modificata: 25 ottobre 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogAppRegistryFullAccess

Descrizione: Fornisce l'accesso completo alle funzionalità del Service Catalog App Registry

AWSServiceCatalogAppRegistryFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSServiceCatalogAppRegistryFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 novembre 2020, 22:25 UTC
- Ora modificata: 07 dicembre 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*:*:*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle funzionalità del registro delle app di Service Catalog

AWSServiceCatalogAppRegistryReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AWSServiceCatalogAppRegistryReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 12 novembre 2020, 22:34 UTC
- Ora modificata: 17 novembre 2022, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogAppRegistryServiceRolePolicy

Descrizione: consente a Service Catalog AppRegistry di gestire Resource Groups per conto dell'utente

AWSServiceCatalogAppRegistryServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 maggio 2021, 22:18 UTC
- Ora modificata: 26 ottobre 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  ]
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogEndUserFullAccess

Descrizione: fornisce l'accesso completo alle funzionalità degli utenti finali del catalogo dei servizi

AWSServiceCatalogEndUserFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSServiceCatalogEndUserFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 febbraio 2018, 17:22 UTC
- Ora modificata: 10 luglio 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogEndUserReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle funzionalità degli utenti finali di Service Catalog

AWSServiceCatalogEndUserReadOnlyAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSServiceCatalogEndUserReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 ottobre 2019, 18:49 UTC
- Ora modificata: 25 ottobre 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Descrizione: una policy Service Linked Role AWS ServiceCatalog per la sincronizzazione con la struttura organizzativa di AWS Organizations

AWSServiceCatalogOrgsDataSyncServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 aprile 2023, 20:48 UTC
- Ora modificata: 10 aprile 2023, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceCatalogSyncServiceRolePolicy

Descrizione: un ruolo collegato al servizio per AWS ServiceCatalog sincronizzare gli artefatti di provisioning dai repository di origine

AWSServiceCatalogSyncServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 15 novembre 2022, 21:20 UTC
- Ora modificata: 03 maggio 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "ArtifactSyncToServiceCatalog",
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:ListProvisioningArtifacts",
      "servicecatalog:DescribeProductAsAdmin",
      "servicecatalog>DeleteProvisioningArtifact",
      "servicecatalog:ListServiceActionsForProvisioningArtifact",
      "servicecatalog:DescribeProvisioningArtifact",
      "servicecatalog>CreateProvisioningArtifact",
      "servicecatalog:UpdateProvisioningArtifact"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AccessArtifactRepositories",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:UseConnection",
      "codeconnections:UseConnection"
    ],
    "Resource" : [
      "arn:aws:codestar-connections:*:*:connection/*",
      "arn:aws:codeconnections:*:*:connection/*"
    ]
  },
  {
    "Sid" : "ValidateTemplate",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ValidateTemplate"
    ],
    "Resource" : "*"
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForAmazonEKSNodegroup

Descrizione: autorizzazioni necessarie per la gestione dei gruppi di nodi nell'account del cliente. Queste politiche si riferivano alla gestione delle seguenti risorse: AutoscalingGroups,, e SecurityGroups. LaunchTemplates InstanceProfiles

AWSServiceRoleForAmazonEKSNodegroup è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 07 novembre 2019, 01:34 UTC
- Ora modificata: 04 gennaio 2024, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
      ]
    }
  }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForAmazonQDeveloper

Descrizione: questo ruolo collegato al servizio offre agli sviluppatori Amazon Q la possibilità di fornire informazioni sull'utilizzo.

AWSServiceRoleForAmazonQDeveloper è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 25 aprile 2024, 07:40 UTC
- Ora modificata: 25 aprile 2024, 07:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
```

```
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/Q"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Descrizione: Fornisce l'accesso alle risorse di Systems Manager utilizzate dagli CloudWatch allarmi

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 1 ottobre 2020, 09:49 UTC
- Ora modificata: 01 ottobre 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

Descrizione: consente di accedere CloudWatch alle metriche di RDS Performance Insights per tuo conto

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 07 settembre 2023, 09:32 UTC
- Ora modificata: 07 settembre 2023, 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForCodeGuru-Profiler

Descrizione: un ruolo collegato al servizio richiesto ad Amazon CodeGuru Profiler per inviare notifiche per tuo conto.

AWSServiceRoleForCodeGuru-Profiler [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 giugno 2020, 22:04 UTC
- Ora modificata: 26 giugno 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForCodeWhispererPolicy

Descrizione: questo ruolo concede le autorizzazioni per accedere CodeWhisperer ai dati del tuo account per calcolare la fatturazione, fornisce l'accesso per creare e accedere ai report di sicurezza in Amazon e CodeGuru inviare dati a CloudWatch

AWSServiceRoleForCodeWhispererPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 marzo 2023, 19:39 UTC
- Ora modificata: 29 marzo 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance",
        "sso:DescribeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
    }
  ]
}
```

```
    "Resource" : [
      "*"
    ],
  },
  {
    "Sid" : "sid4",
    "Effect" : "Allow",
    "Action" : [
      "codeguru-security:CreateScan",
      "codeguru-security:GetScan",
      "codeguru-security:ListFindings",
      "codeguru-security:GetFindings"
    ],
    "Resource" : [
      "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
    ]
  },
  {
    "Sid" : "sid5",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/CodeWhisperer"
        ]
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForEC2ScheduledInstances

Descrizione: consente alle istanze pianificate EC2 di avviare e gestire le istanze spot.

AWSServiceRoleForEC2ScheduledInstances [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 ottobre 2017, 18:31 UTC
- Ora modificata: 12 ottobre 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Descrizione: AWS GroundStation utilizza questo ruolo collegato al servizio per richiamare EC2 per trovare indirizzi IPv4 pubblici

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy [AWS è](#) una politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 13 dicembre 2022, 23:52 UTC
- Ora modificata: 13 dicembre 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForImageBuilder

Descrizione: consente a EC2 ImageBuilder di chiamare AWS i servizi per tuo conto.

AWSServiceRoleForImageBuilder è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 29 novembre 2019, 22:02 UTC
- Ora modificata: 19 ottobre 2023, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Versione della politica

Versione della politica: v19 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:DescribeInstanceState",
        "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-*"
  ]
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForIoTSiteWise

Descrizione: consente SiteWise all' AWS IoT di fornire e gestire gateway e interrogare i dati. La policy include le autorizzazioni AWS Greengrass necessarie per la distribuzione in gruppi, le autorizzazioni AWS Lambda per la creazione e l'aggiornamento di funzioni con prefisso di servizio e le autorizzazioni IoT AWS Analytics per l'interrogazione dei dati dai datastore.

AWSServiceRoleForIoTSiteWise [è una politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 novembre 2018, 19:19 UTC
- Ora modificata: 13 novembre 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
            "IOTSITWISE"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForLogDeliveryPolicy

Descrizione: consente al servizio Log Delivery di fornire i log chiamando la destinazione dei log per conto dell'utente.

AWSServiceRoleForLogDeliveryPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi

- Ora di creazione: 4 ottobre 2019, 17:31 UTC
- Ora modificata: 15 luglio 2021, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForMonitronPolicy

Descrizione: concede ad Amazon Monitron le autorizzazioni per AWS gestire le risorse, AWS inclusa l'assegnazione di utenti SSO per tuo conto.

AWSServiceRoleForMonitronPolicy [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 2 dicembre 2020, 19:06 UTC
- Ora modificata: 29 settembre 2022, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForNeptuneGraphPolicy

Descrizione: Fornisce l'accesso a Cloudwatch per pubblicare parametri e log operativi e di utilizzo per Amazon Neptune

AWSServiceRoleForNeptuneGraphPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 29 novembre 2023, 14:03 UTC
- Ora modificata: 29 novembre 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
  }
}
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Descrizione: fornisce le autorizzazioni per descrivere e aggiornare le risorse di Private Marketplace e descrivere Organizations AWS

AWSServiceRoleForPrivateMarketplaceAdminPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 14 febbraio 2024, 22:28 UTC
- Ora modificata: 14 febbraio 2024, 22:28 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForSMS

Descrizione: fornisce l'accesso ai AWS servizi e alle risorse necessari per migrare le istanze di servizio AWS tra cui EC2, S3 e Cloudformation.

AWSServiceRoleForSMS [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 6 agosto 2019, 18:39 UTC
- Ora modificata: 15 ottobre 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRoleForUserSubscriptions

Descrizione: fornisce l'accesso al servizio User Subscriptions alle risorse dell'Identity Center per aggiornare automaticamente le sottoscrizioni.

AWSServiceRoleForUserSubscriptions è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 25 aprile 2024, 16:14 UTC
- Ora modificata: 25 aprile 2024, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SubscriptionManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "organizations:DescribeOrganization",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRolePolicyForBackupReports

Descrizione: Fornisce autorizzazioni di AWS Backup per creare report di conformità per tuo conto

AWSServiceRolePolicyForBackupReports è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 agosto 2021, 21:16 UTC
- Ora modificata: 10 marzo 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSServiceRolePolicyForBackupRestoreTesting

Descrizione: questa politica contiene le autorizzazioni per testare i ripristini e per ripulire le risorse create durante i test.

AWSServiceRolePolicyForBackupRestoreTesting è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 novembre 2023, 23:37 UTC
- Ora modificata: 14 febbraio 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSShieldDRTAccessPolicy

Descrizione: fornisce al AWS DDoS Response Team un accesso limitato alle vostre risorse per aiutarvi Account AWS a mitigare gli attacchi DDoS durante un evento di elevata gravità.

AWSShieldDRTAccessPolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSShieldDRTAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2018, 22:29 UTC

- Ora modificata: 15 dicembre 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSShieldServiceRolePolicy

Descrizione: consente a AWS Shield di accedere alle AWS risorse per tuo conto per fornire protezione DDoS.

AWSShieldServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 novembre 2021, 19:17 UTC
- Ora modificata: 17 novembre 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSSMForSAPServiceLinkedRolePolicy

Descrizione: fornisce a AWS Systems Manager for SAP le autorizzazioni necessarie per gestire e integrare il software SAP con. AWS

AWSSSMForSAPServiceLinkedRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 novembre 2022, 01:18 UTC
- Ora modificata: 11 aprile 2024, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:aws:events:::*:rule/SSMSAPManagedRule*",
      "arn:aws:events:::*:event-bus/default"
    ]
  },
  {
    "Sid" : "DocumentActions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ssm::*:document/AWSSystemsManagerSAP-*",
      "arn:aws:ssm::*:document/AWSSSMSAP*",
      "arn:aws:ssm::*:document/AWSSAP*"
    ]
  },
  {
    "Sid" : "CustomerSendCommand",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : "arn:aws: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_*"
      ]
    },
    {
      "Sid" : "StartStopInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSSMOpsInsightsServiceRolePolicy

Descrizione: Policy for Service Linked Role AWSServiceRoleForAmazonSSM_OpsInsights

AWSSSMOpsInsightsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 giugno 2021, 20:12 UTC
- Ora modificata: 16 giugno 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSSODirectoryAdministrator

Descrizione: accesso da amministratore per SSO Directory

AWSSSODirectoryAdministrator è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSSODirectoryAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 31 ottobre 2018, 23:54 UTC
- Ora modificata: 20 ottobre 2022, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSSODirectoryReadOnly

Descrizione: ReadOnly accesso per SSO Directory

AWSSSODirectoryReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSSODirectoryReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 31 ottobre 2018, 23:49 UTC
- Ora modificata: 16 novembre 2022, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSSOMasterAccountAdministrator

Descrizione: Fornisce l'accesso all'interno dell' AWS SSO per gestire gli account master e membri di AWS Organizations e l'applicazione cloud

AWSSSOMasterAccountAdministrator è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSSOMasterAccountAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2018, 20:36 UTC
- Ora modificata: 26 aprile 2024, 00:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
```

```

        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSSSOManageDelegatedAdministrator",
    "Effect" : "Allow",
    "Action" : [
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "sso.amazonaws.com"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSSOMemberAccountAdministrator

Descrizione: Fornisce l'accesso all'interno dell' AWS SSO per gestire gli account dei membri di AWS Organizations e l'applicazione cloud

AWSSSOMemberAccountAdministrator è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSSOMemberAccountAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2018, 20:45 UTC
- Ora modificata: 26 aprile 2024, 00:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Sid" : "AWSSSOMemberAccountAdministrator",
    "Effect" : "Allow",
    "Action" : [
      "ds:DescribeDirectories",
      "ds:AuthorizeApplication",
      "ds:UnauthorizeApplication",
      "ds:DescribeTrusts",
      "iam:ListPolicies",
      "organizations:EnableAWSServiceAccess",
      "organizations:DescribeOrganization",
      "organizations:DescribeAccount",
      "organizations:ListRoots",
      "organizations:ListAccounts",
      "organizations:ListAccountsForParent",
      "organizations:ListParents",
      "organizations:ListChildren",
      "organizations:ListOrganizationalUnitsForParent",
      "organizations:ListDelegatedAdministrators",
      "sso:*",
      "sso-directory:*",
      "identitystore:*",
      "identitystore-auth:*",
      "ds:CreateAlias",
      "access-analyzer:ValidatePolicy",
      "signin:CreateTrustedIdentityPropagationApplicationForConsole",
      "signin:ListTrustedIdentityPropagationApplicationsForConsole"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSSSOManageDelegatedAdministrator",
    "Effect" : "Allow",
    "Action" : [
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "sso.amazonaws.com"
      }
    }
  }
]
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSS0ReadOnly

Descrizione: fornisce accesso in sola lettura alle configurazioni AWS SSO.

AWSSS0ReadOnly è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSS0ReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2018, 20:24 UTC
- Ora modificata: 26 aprile 2024, 00:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSS0ReadOnly`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSSOServiceRolePolicy

Descrizione: concede le autorizzazioni AWS SSO per gestire le AWS risorse, inclusi ruoli IAM, policy e IdP SAML per tuo conto.

AWSSSOServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 dicembre 2017, 18:36 UTC
- Ora modificata: 20 ottobre 2022, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Versione della politica

Versione della politica: v17 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
```

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSStepFunctionsConsoleFullAccess

Descrizione: una politica di accesso per fornire un accesso utente/ruolo/ecc alla console. AWS StepFunctions Per un'esperienza completa con la console, oltre a questa policy, un utente potrebbe aver bisogno di iam: PassRole autorizzazione per altri ruoli IAM che può essere assunta dal servizio.

AWSStepFunctionsConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSStepFunctionsConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 gennaio 2017, 21:54 UTC
- Ora modificata: 12 gennaio 2017, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSStepFunctionsFullAccess

Descrizione: una politica di accesso per fornire un accesso utente/ruolo/etc all'API. AWS StepFunctions Per un accesso completo, oltre a questa politica, un utente DEVE disporre dell'PassRole autorizzazione iam: su almeno un ruolo IAM che può essere assunto dal servizio.

AWSStepFunctionsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSStepFunctionsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 gennaio 2017, 21:51 UTC
- Ora modificata: 11 gennaio 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSStepFunctionsReadOnlyAccess

Descrizione: una politica di accesso per fornire a un utente/ruolo/ecc l'accesso in sola lettura al servizio. AWS StepFunctions

AWSStepFunctionsReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSStepFunctionsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 gennaio 2017, 21:46 UTC
- Ora modificata: 26 aprile 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "ReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "states:ListStateMachines",
      "states:ListActivities",
      "states:DescribeStateMachine",
      "states:DescribeStateMachineForExecution",
      "states:ListExecutions",
      "states:DescribeExecution",
      "states:GetExecutionHistory",
      "states:DescribeActivity",
      "states:ListTagsForResource",
      "states:DescribeMapRun",
      "states:ListMapRuns",
      "states:DescribeStateMachineAlias",
      "states:ListStateMachineAliases",
      "states:ListStateMachineVersions",
      "states:ValidateStateMachineDefinition"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSStorageGatewayFullAccess

Descrizione: fornisce l'accesso completo a AWS Storage Gateway tramite AWS Management Console.

AWSStorageGatewayFullAccess è una [policy AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSStorageGatewayFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 06 settembre 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSStorageGatewayReadOnlyAccess

Descrizione: fornisce l'accesso a AWS Storage Gateway tramite AWS Management Console.

AWSStorageGatewayReadOnlyAccess è una [policy AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSStorageGatewayReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 06 settembre 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSStorageGatewayServiceRolePolicy

Descrizione: ruolo collegato ai servizi utilizzato da AWS Storage Gateway per consentire l'integrazione di altri AWS servizi con Storage Gateway.

AWSStorageGatewayServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 febbraio 2021, 19:03 UTC
- Ora modificata: 17 febbraio 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    "Resource" : "arn:aws:fsx:*:*:backup/*"
  }
]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSupplyChainFederationAdminAccess

Descrizione: AWSSupplyChainFederationAdminAccess fornisce agli utenti federati di AWS Supply Chain l'accesso all'applicazione AWS Supply Chain, incluse le autorizzazioni necessarie per eseguire azioni all'interno dell'applicazione AWS Supply Chain. La policy fornisce autorizzazioni amministrative per gli utenti e i gruppi di IAM Identity Center ed è associata a un ruolo creato da AWS Supply Chain per tuo conto. Non dovresti collegare la AWSSupplyChainFederationAdminAccess policy a nessun'altra entità IAM.

AWSSupplyChainFederationAdminAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSupplyChainFederationAdminAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 marzo 2023, 18:54 UTC
- Ora modificata: 01 novembre 2023, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSupportAccess

Descrizione: consente agli utenti di accedere al AWS Support Centro.

AWSSupportAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSupportAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSupportAppFullAccess

Descrizione: Fornisce l'accesso completo all' AWS Support App e ad altri servizi richiesti, come AWS Support Service Quotas. Questa politica include le autorizzazioni per utilizzare i servizi di supporto in modo che l'utente possa contattarli AWS Support per casi di assistenza, modificare le quote di servizio e creare i ruoli pertinenti collegati ai servizi.

AWSSupportAppFullAccess è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti `AWSSupportAppFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 agosto 2022, 16:53 UTC
- Ora modificata: 22 agosto 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSupportAppReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura all' AWS Support app.

AWSSupportAppReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSupportAppReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 agosto 2022, 17:01 UTC
- Ora modificata: 22 agosto 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSupportPlansFullAccess

Descrizione: fornisce l'accesso completo ai piani di supporto.

AWSSupportPlansFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSupportPlansFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 settembre 2022, 18:19 UTC
- Ora modificata: 09 maggio 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSupportPlansReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ai piani di supporto.

AWSSupportPlansReadOnlyAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSSupportPlansReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 settembre 2022, 18:08 UTC
- Ora modificata: 27 settembre 2022, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
      ]
    }
  ]
}
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSupportServiceRolePolicy

Descrizione: consente di accedere AWS Support alle AWS risorse per fornire servizi di fatturazione, amministrazione e supporto.

AWSSupportServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 aprile 2018, 18:04 UTC
- Ora modificata: 02 maggio 2024, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Versione della politica

Versione della politica: v36 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:describeScraper",
"aps:describeWorkspace",
"aps:listRuleGroupsNamespaces",
"aps:listScrapers",
"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:getRestoreJobMetadata",
"backup:getRestoreTestingInferredMetadata",
"backup:getRestoreTestingPlan",
"backup:getRestoreTestingSelection",
"backup:getSupportedResourceTypes",
"backup:listBackupJobs",
"backup:listBackupPlans",
"backup:listBackupPlanTemplates",
"backup:listBackupPlanVersions",
"backup:listBackupSelections",
"backup:listBackupVaults",
"backup:listCopyJobs",
"backup:listFrameworks",
"backup:listLegalHolds",
"backup:listProtectedResources",
"backup:listRecoveryPointsByBackupVault",
```

```
"backup:listRecoveryPointsByLegalHold",
"backup:listRecoveryPointsByResource",
"backup:listReportJobs",
"backup:listReportPlans",
"backup:listRestoreJobs",
"backup:listRestoreJobsByProtectedResource",
"backup:listRestoreTestingPlans",
"backup:listRestoreTestingSelections",
"backup:listTags",
"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:getResponseHeadersPolicy",
"cloudfront:getResponseHeadersPolicyConfig",
"cloudfront:getStreamingDistribution",
"cloudfront:getStreamingDistributionConfig",
"cloudfront:listCachePolicies",
"cloudfront:listCloudFrontOriginAccessIdentities",
"cloudfront:listContinuousDeploymentPolicies",
"cloudfront:listDistributions",
"cloudfront:listDistributionsByCachePolicyId",
"cloudfront:listDistributionsByKeyGroup",
"cloudfront:listDistributionsByOriginRequestPolicyId",
"cloudfront:listDistributionsByRealtimeLogConfig",
"cloudfront:listDistributionsByResponseHeadersPolicyId",
"cloudfront:listDistributionsByWebACLId",
"cloudfront:listFunctions",
"cloudfront:listInvalidations",
"cloudfront:listKeyGroups",
"cloudfront:listOriginAccessControls",
"cloudfront:listOriginRequestPolicies",
"cloudfront:listPublicKeys",
"cloudfront:listRealtimeLogConfigs",
"cloudfront:listResponseHeadersPolicies",
"cloudfront:listStreamingDistributions",
"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:batchGetFleets",
"codebuild:batchGetProjects",
"codebuild:listBuildBatches",
"codebuild:listBuildBatchesForProject",
"codebuild:listBuilds",
"codebuild:listBuildsForProject",
"codebuild:listCuratedEnvironmentImages",
"codebuild:listFleets",
"codebuild:listProjects",
"codebuild:listSourceCredentials",
"codecommit:batchGetRepositories",
"codecommit:getBranch",
"codecommit:getRepository",
"codecommit:getRepositoryTriggers",
```

```
"codecommit:listBranches",
"codecommit:listRepositories",
"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:getLandingZone",
"controltower:getLandingZoneStatus",
```

```
"controltower:listDirectoryGroups",
"controltower:listEnabledControls",
"controltower:listGuardrailsForTarget",
"controltower:listGuardrailViolations",
"controltower:listLandingZones",
"controltower:listManagedAccounts",
"controltower:listManagedAccountsForGuardrail",
"controltower:listManagedAccountsForParent",
"controltower:listManagedOrganizationalUnits",
"controltower:listManagedOrganizationalUnitsForGuardrail",
"cost-optimization-hub:getPreferences",
"cost-optimization-hub:getRecommendation",
"cost-optimization-hub:listEnrollmentStatuses",
"cost-optimization-hub:listRecommendations",
"cost-optimization-hub:listRecommendationSummaries",
"databrew:describeDataset",
"databrew:describeJob",
"databrew:describeProject",
"databrew:describeRecipe",
"databrew:listDatasets",
"databrew:listJobRuns",
"databrew:listJobs",
"databrew:listProjects",
"databrew:listRecipes",
"databrew:listRecipeVersions",
"databrew:listTagsForResource",
"datapipeline:describeObjects",
"datapipeline:describePipelines",
"datapipeline:getPipelineDefinition",
"datapipeline:listPipelines",
"datapipeline:queryObjects",
"datasync:describeAgent",
"datasync: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",
"dms:getLifecyclePolicies",
"dms:getLifecyclePolicy",
"dms:describeAccountAttributes",
"dms:describeApplicableIndividualAssessments",
"dms:describeConnections",
"dms:describeEndpoints",
"dms:describeEndpointSettings",
"dms:describeEndpointTypes",
"dms:describeEventCategories",
"dms:describeEvents",
"dms:describeEventSubscriptions",
"dms:describeFleetAdvisorCollectors",
"dms:describeFleetAdvisorDatabases",
"dms:describeFleetAdvisorLsaAnalysis",
"dms:describeFleetAdvisorSchemaObjectSummary",
"dms:describeFleetAdvisorSchemas",
"dms:describeOrderableReplicationInstances",
"dms:describePendingMaintenanceActions",
"dms:describeRefreshSchemasStatus",
"dms:describeReplicationInstances",
"dms:describeReplicationInstanceTaskLogs",
"dms:describeReplicationSubnetGroups",
"dms:describeReplicationTaskAssessmentResults",
"dms:describeReplicationTaskAssessmentRuns",
"dms:describeReplicationTaskIndividualAssessments",
"dms:describeReplicationTasks",
"dms:describeSchemas",
"dms:describeTableStatistics",
"docdb-elastic:getCluster",
```

```
"docdb-elastic:getClusterSnapshot",
"docdb-elastic:listClusters",
"docdb-elastic:listClusterSnapshots",
"dms:describeJobLogItems",
"dms:describeJobs",
"dms:describeLaunchConfigurationTemplates",
"dms:describeRecoveryInstances",
"dms:describeRecoverySnapshots",
"dms:describeReplicationConfigurationTemplates",
"dms:describeSourceNetworks",
"dms:describeSourceServers",
"dms:getLaunchConfiguration",
"dms:getReplicationConfiguration",
"dms:listExtensibleSourceServers",
"dms:listLaunchActions",
"dms:listStagingAccounts",
"ds:describeClientAuthenticationSettings",
"ds:describeConditionalForwarders",
"ds:describeDirectories",
"ds:describeDomainControllers",
"ds:describeEventTopics",
"ds:describeLDAPSSettings",
"ds:describeSharedDirectories",
"ds:describeSnapshots",
"ds:describeTrusts",
"ds:getDirectoryLimits",
"ds:getSnapshotLimits",
"ds:listIpRoutes",
"ds:listSchemaExtensions",
"ds:listTagsForResource",
"dynamodb:describeBackup",
"dynamodb:describeContinuousBackups",
"dynamodb:describeContributorInsights",
"dynamodb:describeExport",
"dynamodb:describeGlobalTable",
"dynamodb:describeImport",
"dynamodb:describeKinesisStreamingDestination",
"dynamodb:describeLimits",
"dynamodb:describeStream",
"dynamodb:describeTable",
"dynamodb:describeTimeToLive",
"dynamodb:listBackups",
"dynamodb:listContributorInsights",
"dynamodb:listExports",
```

```
"dynamodb:listGlobalTables",
"dynamodb:listImports",
"dynamodb:listStreams",
"dynamodb:listTables",
"dynamodb:listTagsOfResource",
"ec2:describeAccountAttributes",
"ec2:describeAddresses",
"ec2:describeAddressesAttribute",
"ec2:describeAddressTransfers",
"ec2:describeAggregateIdFormat",
"ec2:describeAvailabilityZones",
"ec2:describeBundleTasks",
"ec2:describeByoipCidrs",
"ec2:describeCapacityReservationFleets",
"ec2:describeCapacityReservations",
"ec2:describeCarrierGateways",
"ec2:describeClassicLinkInstances",
"ec2:describeClientVpnAuthorizationRules",
"ec2:describeClientVpnConnections",
"ec2:describeClientVpnEndpoints",
"ec2:describeClientVpnRoutes",
"ec2:describeClientVpnTargetNetworks",
"ec2:describeCoipPools",
"ec2:describeConversionTasks",
"ec2:describeCustomerGateways",
"ec2:describeDhcpOptions",
"ec2:describeEgressOnlyInternetGateways",
"ec2:describeExportImageTasks",
"ec2:describeExportTasks",
"ec2:describeFastLaunchImages",
"ec2:describeFastSnapshotRestores",
"ec2:describeFleetHistory",
"ec2:describeFleetInstances",
"ec2:describeFleets",
"ec2:describeFlowLogs",
"ec2:describeFpgaImageAttribute",
"ec2:describeFpgaImages",
"ec2:describeHostReservationOfferings",
"ec2:describeHostReservations",
"ec2:describeHosts",
"ec2:describeIamInstanceProfileAssociations",
"ec2:describeIdentityIdFormat",
"ec2:describeIdFormat",
"ec2:describeImageAttribute",
```

```
"ec2:describeImages",
"ec2:describeImportImageTasks",
"ec2:describeImportSnapshotTasks",
"ec2:describeInstanceAttribute",
"ec2:describeInstanceCreditSpecifications",
"ec2:describeInstanceEventNotificationAttributes",
"ec2:describeInstanceEventWindows",
"ec2:describeInstances",
"ec2:describeInstanceStatus",
"ec2:describeInstanceTypeOfferings",
"ec2:describeInstanceTypes",
"ec2:describeInternetGateways",
"ec2:describeIpamPools",
"ec2:describeIpams",
"ec2:describeIpamScopes",
"ec2:describeIpv6Pools",
"ec2:describeKeyPairs",
"ec2:describeLaunchTemplates",
"ec2:describeLaunchTemplateVersions",
"ec2:describeLocalGatewayRouteTables",
"ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:describeLocalGatewayRouteTableVpcAssociations",
"ec2:describeLocalGateways",
"ec2:describeLocalGatewayVirtualInterfaceGroups",
"ec2:describeLocalGatewayVirtualInterfaces",
"ec2:describeManagedPrefixLists",
"ec2:describeMovingAddresses",
"ec2:describeNatGateways",
"ec2:describeNetworkAcls",
"ec2:describeNetworkInterfaceAttribute",
"ec2:describeNetworkInterfaces",
"ec2:describePlacementGroups",
"ec2:describePrefixLists",
"ec2:describePrincipalIdFormat",
"ec2:describePublicIpv4Pools",
"ec2:describeRegions",
"ec2:describeReservedInstances",
"ec2:describeReservedInstancesListings",
"ec2:describeReservedInstancesModifications",
"ec2:describeReservedInstancesOfferings",
"ec2:describeRouteTables",
"ec2:describeScheduledInstanceAvailability",
"ec2:describeScheduledInstances",
"ec2:describeSecurityGroupReferences",
```



```
"ec2:describeSecurityGroupRules",
"ec2:describeSecurityGroups",
"ec2:describeSnapshotAttribute",
"ec2:describeSnapshots",
"ec2:describeSpotDatafeedSubscription",
"ec2:describeSpotFleetInstances",
"ec2:describeSpotFleetRequestHistory",
"ec2:describeSpotFleetRequests",
"ec2:describeSpotInstanceRequests",
"ec2:describeSpotPriceHistory",
"ec2:describeStaleSecurityGroups",
"ec2:describeStoreImageTasks",
"ec2:describeSubnets",
"ec2:describeTags",
"ec2:describeTrafficMirrorFilters",
"ec2:describeTrafficMirrorSessions",
"ec2:describeTrafficMirrorTargets",
"ec2:describeTransitGatewayAttachments",
"ec2:describeTransitGatewayConnectPeers",
"ec2:describeTransitGatewayMulticastDomains",
"ec2:describeTransitGatewayPeeringAttachments",
"ec2:describeTransitGatewayPolicyTables",
"ec2:describeTransitGatewayRouteTableAnnouncements",
"ec2:describeTransitGatewayRouteTables",
"ec2:describeTransitGateways",
"ec2:describeTransitGatewayVpcAttachments",
"ec2:describeVerifiedAccessEndpoints",
"ec2:describeVerifiedAccessGroups",
"ec2:describeVerifiedAccessInstances",
"ec2:describeVerifiedAccessTrustProviders",
"ec2:describeVolumeAttribute",
"ec2:describeVolumes",
"ec2:describeVolumesModifications",
"ec2:describeVolumeStatus",
"ec2:describeVpcAttribute",
"ec2:describeVpcClassicLink",
"ec2:describeVpcClassicLinkDnsSupport",
"ec2:describeVpcEndpointConnectionNotifications",
"ec2:describeVpcEndpointConnections",
"ec2:describeVpcEndpoints",
"ec2:describeVpcEndpointServiceConfigurations",
"ec2:describeVpcEndpointServicePermissions",
"ec2:describeVpcEndpointServices",
"ec2:describeVpcPeeringConnections",
```

```
"ec2:describeVpcs",
"ec2:describeVpnConnections",
"ec2:describeVpnGateways",
"ec2:getAssociatedIpv6PoolCidrs",
"ec2:getCapacityReservationUsage",
"ec2:getCoipPoolUsage",
"ec2:getConsoleOutput",
"ec2:getConsoleScreenshot",
"ec2:getDefaultCreditSpecification",
"ec2:getEbsDefaultKmsKeyId",
"ec2:getEbsEncryptionByDefault",
"ec2:getGroupsForCapacityReservation",
"ec2:getHostReservationPurchasePreview",
"ec2:getInstanceTypesFromInstanceRequirements",
"ec2:getIpamAddressHistory",
"ec2:getIpamPoolAllocations",
"ec2:getIpamPoolCidrs",
"ec2:getIpamResourceCidrs",
"ec2:getLaunchTemplateData",
"ec2:getManagedPrefixListAssociations",
"ec2:getManagedPrefixListEntries",
"ec2:getReservedInstancesExchangeQuote",
"ec2:getSerialConsoleAccessStatus",
"ec2:getSpotPlacementScores",
"ec2:getTransitGatewayMulticastDomainAssociations",
"ec2:getTransitGatewayPrefixListReferences",
"ec2:getVerifiedAccessEndpointPolicy",
"ec2:getVerifiedAccessGroupPolicy",
"ec2:listImagesInRecycleBin",
"ec2:listSnapshotsInRecycleBin",
"ec2:searchLocalGatewayRoutes",
"ec2:searchTransitGatewayMulticastGroups",
"ec2:searchTransitGatewayRoutes",
"ecr-public:describeImages",
"ecr-public:describeImageTags",
"ecr-public:describeRegistries",
"ecr-public:describeRepositories",
"ecr-public:getRegistryCatalogData",
"ecr-public:getRepositoryCatalogData",
"ecr-public:getRepositoryPolicy",
"ecr-public:listTagsForResource",
"ecr:batchCheckLayerAvailability",
"ecr:batchGetRepositoryScanningConfiguration",
"ecr:describeImages",
```

```
"ecr:describeImageReplicationStatus",
"ecr:describeImageScanFindings",
"ecr:describePullThroughCacheRules",
"ecr:describeRegistry",
"ecr:describeRepositories",
"ecr:getLifecyclePolicy",
"ecr:getLifecyclePolicyPreview",
"ecr:getRegistryPolicy",
"ecr:getRegistryScanningConfiguration",
"ecr:getRepositoryPolicy",
"ecr:listImages",
"ecr:listTagsForResource",
"ecs:describeCapacityProviders",
"ecs:describeClusters",
"ecs:describeContainerInstances",
"ecs:describeServices",
"ecs:describeTaskDefinition",
"ecs:describeTasks",
"ecs:describeTaskSets",
"ecs:getTaskProtection",
"ecs:listAccountSettings",
"ecs:listAttributes",
"ecs:listClusters",
"ecs:listContainerInstances",
"ecs:listServices",
"ecs:listServicesByNamespace",
"ecs:listTagsForResource",
"ecs:listTaskDefinitionFamilies",
"ecs:listTaskDefinitions",
"ecs:listTasks",
"eks:describeAccessEntry",
"eks:describeAddon",
"eks:describeAddonConfiguration",
"eks:describeAddonVersions",
"eks:describeCluster",
"eks:describeEksAnywhereSubscription",
"eks:describeFargateProfile",
"eks:describeIdentityProviderConfig",
"eks:describeNodegroup",
"eks:describeUpdate",
"eks:listAccessEntries",
"eks:listAccessPolicies",
"eks:listAddons",
"eks:listAssociatedAccessPolicies",
```

```
"eks:listClusters",
"eks:listEksAnywhereSubscriptions",
"eks:listFargateProfiles",
"eks:listIdentityProviderConfigs",
"eks:listNodegroups",
"eks:listUpdates",
"elasticache:describeCacheClusters",
"elasticache:describeCacheEngineVersions",
"elasticache:describeCacheParameterGroups",
"elasticache:describeCacheParameters",
"elasticache:describeCacheSecurityGroups",
"elasticache:describeCacheSubnetGroups",
"elasticache:describeEngineDefaultParameters",
"elasticache:describeEvents",
"elasticache:describeGlobalReplicationGroups",
"elasticache:describeReplicationGroups",
"elasticache:describeReservedCacheNodes",
"elasticache:describeReservedCacheNodesOfferings",
"elasticache:describeServerlessCaches",
"elasticache:describeServerlessCacheSnapshots",
"elasticache:describeServiceUpdates",
"elasticache:describeSnapshots",
"elasticache:describeUpdateActions",
"elasticache:describeUserGroups",
"elasticache:describeUsers",
"elasticache:listAllowedNodeTypeModifications",
"elasticache:listTagsForResource",
"elasticbeanstalk:checkDNSAvailability",
"elasticbeanstalk:describeAccountAttributes",
"elasticbeanstalk:describeApplicationVersions",
"elasticbeanstalk:describeApplications",
"elasticbeanstalk:describeConfigurationOptions",
"elasticbeanstalk:describeEnvironmentHealth",
"elasticbeanstalk:describeEnvironmentManagedActionHistory",
"elasticbeanstalk:describeEnvironmentManagedActions",
"elasticbeanstalk:describeEnvironmentResources",
"elasticbeanstalk:describeEnvironments",
"elasticbeanstalk:describeEvents",
"elasticbeanstalk:describeInstancesHealth",
"elasticbeanstalk:describePlatformVersion",
"elasticbeanstalk:listAvailableSolutionStacks",
"elasticbeanstalk:listPlatformBranches",
"elasticbeanstalk:listPlatformVersions",
"elasticbeanstalk:validateConfigurationSettings",
```

```
"elasticfilesystem:describeAccessPoints",
"elasticfilesystem:describeFileSystemPolicy",
"elasticfilesystem:describeFileSystems",
"elasticfilesystem:describeLifecycleConfiguration",
"elasticfilesystem:describeMountTargets",
"elasticfilesystem:describeMountTargetSecurityGroups",
"elasticfilesystem:describeTags",
"elasticfilesystem:listTagsForResource",
"elasticloadbalancing:describeAccountLimits",
"elasticloadbalancing:describeInstanceHealth",
"elasticloadbalancing:describeListenerCertificates",
"elasticloadbalancing:describeListeners",
"elasticloadbalancing:describeLoadBalancerAttributes",
"elasticloadbalancing:describeLoadBalancerPolicies",
"elasticloadbalancing:describeLoadBalancerPolicyTypes",
"elasticloadbalancing:describeLoadBalancers",
"elasticloadbalancing:describeRules",
"elasticloadbalancing:describeSSLPolicies",
"elasticloadbalancing:describeTags",
"elasticloadbalancing:describeTargetGroupAttributes",
"elasticloadbalancing:describeTargetGroups",
"elasticloadbalancing:describeTargetHealth",
"elasticmapreduce:describeCluster",
"elasticmapreduce:describeNotebookExecution",
"elasticmapreduce:describeReleaseLabel",
"elasticmapreduce:describeSecurityConfiguration",
"elasticmapreduce:describeStep",
"elasticmapreduce:describeStudio",
"elasticmapreduce:getAutoTerminationPolicy",
"elasticmapreduce:getBlockPublicAccessConfiguration",
"elasticmapreduce:getManagedScalingPolicy",
"elasticmapreduce:getStudioSessionMapping",
"elasticmapreduce:listBootstrapActions",
"elasticmapreduce:listClusters",
"elasticmapreduce:listInstanceFleets",
"elasticmapreduce:listInstanceGroups",
"elasticmapreduce:listInstances",
"elasticmapreduce:listNotebookExecutions",
"elasticmapreduce:listReleaseLabels",
"elasticmapreduce:listSecurityConfigurations",
"elasticmapreduce:listSteps",
"elasticmapreduce:listStudios",
"elasticmapreduce:listStudioSessionMappings",
"elastictranscoder:listJobsByPipeline",
```

```
"elastictranscoder:listJobsByStatus",
"elastictranscoder:listPipelines",
"elastictranscoder:listPresets",
"elastictranscoder:readPipeline",
"elastictranscoder:readPreset",
"emr-containers:describeJobRun",
"emr-containers:describeJobTemplate",
"emr-containers:describeManagedEndpoint",
"emr-containers:describeVirtualCluster",
"emr-containers:listJobRuns",
"emr-containers:listJobTemplates",
"emr-containers:listManagedEndpoints",
"emr-containers:listVirtualClusters",
"emr-serverless:getApplication",
"emr-serverless:getJobRun",
"emr-serverless:listApplications",
"es:describeDomain",
"es:describeDomainAutoTunes",
"es:describeDomainChangeProgress",
"es:describeDomainConfig",
"es:describeDomains",
"es:describeDryRunProgress",
"es:describeElasticsearchDomain",
"es:describeElasticsearchDomainConfig",
"es:describeElasticsearchDomains",
"es:describeInboundConnections",
"es:describeInstanceTypeLimits",
"es:describeOutboundConnections",
"es:describePackages",
"es:describeReservedInstanceOfferings",
"es:describeReservedInstances",
"es:describeVpcEndpoints",
"es:getCompatibleVersions",
"es:getPackageVersionHistory",
"es:getUpgradeHistory",
"es:getUpgradeStatus",
"es:listDomainNames",
"es:listDomainsForPackage",
"es:listInstanceTypeDetails",
"es:listPackagesForDomain",
"es:listScheduledActions",
"es:listTags",
"es:listVersions",
"es:listVpcEndpointAccess",
```

```
"es:listVpcEndpoints",
"es:listVpcEndpointsForDomain",
"evidently:getExperiment",
"evidently:getFeature",
"evidently:getLaunch",
"evidently:getProject",
"evidently:getSegment",
"evidently:listExperiments",
"evidently:listFeatures",
"evidently:listLaunches",
"evidently:listProjects",
"evidently:listSegments",
"evidently:listSegmentReferences",
"events:describeApiDestination",
"events:describeArchive",
"events:describeConnection",
"events:describeEndpoint",
"events:describeEventBus",
"events:describeEventSource",
"events:describePartnerEventSource",
"events:describeReplay",
"events:describeRule",
"events:listArchives",
"events:listApiDestinations",
"events:listConnections",
"events:listEndpoints",
"events:listEventBuses",
"events:listEventSources",
"events:listPartnerEventSourceAccounts",
"events:listPartnerEventSources",
"events:listReplays",
"events:listRuleNamesByTarget",
"events:listRules",
"events:listTargetsByRule",
"events:testEventPattern",
"firehose:describeDeliveryStream",
"firehose:listDeliveryStreams",
"fms:getAdminAccount",
"fms:getComplianceDetail",
"fms:getNotificationChannel",
"fms:getPolicy",
"fms:getProtectionStatus",
"fms:listComplianceStatus",
"fms:listMemberAccounts",
```

```
"fms:listPolicies",
"forecast:describeDataset",
"forecast:describeDatasetGroup",
"forecast:describeDatasetImportJob",
"forecast:describeForecast",
"forecast:describeForecastExportJob",
"forecast:describePredictor",
"forecast:getAccuracyMetrics",
"forecast:listDatasetGroups",
"forecast:listDatasetImportJobs",
"forecast:listDatasets",
"forecast:listForecastExportJobs",
"forecast:listForecasts",
"forecast:listPredictors",
"fsx:describeBackups",
"fsx:describeDataRepositoryAssociations",
"fsx:describeDataRepositoryTasks",
"fsx:describeFileCaches",
"fsx:describeFileSystems",
"fsx:describeSnapshots",
"fsx:describeStorageVirtualMachines",
"fsx:describeVolumes",
"fsx:listTagsForResource",
"gamelift:describeAlias",
"gamelift:describeBuild",
"gamelift:describeEC2InstanceLimits",
"gamelift:describeFleetAttributes",
"gamelift:describeFleetCapacity",
"gamelift:describeFleetEvents",
"gamelift:describeFleetLocationAttributes",
"gamelift:describeFleetLocationCapacity",
"gamelift:describeFleetLocationUtilization",
"gamelift:describeFleetPortSettings",
"gamelift:describeFleetUtilization",
"gamelift:describeGameServer",
"gamelift:describeGameServerGroup",
"gamelift:describeGameSessionDetails",
"gamelift:describeGameSessionPlacement",
"gamelift:describeGameSessionQueues",
"gamelift:describeGameSessions",
"gamelift:describeInstances",
"gamelift:describeMatchmaking",
"gamelift:describeMatchmakingConfigurations",
"gamelift:describeMatchmakingRuleSets",
```



```
"gamelift:describePlayerSessions",
"gamelift:describeRuntimeConfiguration",
"gamelift:describeScalingPolicies",
"gamelift:describeScript",
"gamelift:listAliases",
"gamelift:listBuilds",
"gamelift:listFleets",
"gamelift:listGameServerGroups",
"gamelift:listGameServers",
"gamelift:listScripts",
"gamelift:resolveAlias",
"glacier:describeJob",
"glacier:describeVault",
"glacier:getDataRetrievalPolicy",
"glacier:getVaultAccessPolicy",
"glacier:getVaultLock",
"glacier:getVaultNotifications",
"glacier:listJobs",
"glacier:listTagsForVault",
"glacier:listVaults",
"globalaccelerator:describeAccelerator",
"globalaccelerator:describeAcceleratorAttributes",
"globalaccelerator:describeEndpointGroup",
"globalaccelerator:describeListener",
"globalaccelerator:listAccelerators",
"globalaccelerator:listEndpointGroups",
"globalaccelerator:listListeners",
"glue:batchGetBlueprints",
"glue:batchGetCrawlers",
"glue:batchGetDevEndpoints",
"glue:batchGetJobs",
"glue:batchGetPartition",
"glue:batchGetTriggers",
"glue:batchGetWorkflows",
"glue:checkSchemaVersionValidity",
"glue:getBlueprint",
"glue:getBlueprintRun",
"glue:getBlueprintRuns",
"glue:getCatalogImportStatus",
"glue:getClassifier",
"glue:getClassifiers",
"glue:getColumnStatisticsForPartition",
"glue:getColumnStatisticsForTable",
"glue:getCrawler",
```

```
"glue:getCrawlerMetrics",
"glue:getCrawlers",
"glue:getCustomEntityType",
"glue:getDatabase",
"glue:getDatabases",
"glue:getDataflowGraph",
"glue:getDataQualityResult",
"glue:getDataQualityRuleRecommendationRun",
"glue:getDataQualityRuleset",
"glue:getDataQualityRulesetEvaluationRun",
"glue:getDevEndpoint",
"glue:getDevEndpoints",
"glue:getJob",
"glue:getJobRun",
"glue:getJobRuns",
"glue:getJobs",
"glue:getMapping",
"glue:getMLTaskRun",
"glue:getMLTaskRuns",
"glue:getMLTransform",
"glue:getMLTransforms",
"glue:getPartition",
"glue:getPartitionIndexes",
"glue:getPartitions",
"glue:getRegistry",
"glue:getResourcePolicies",
"glue:getResourcePolicy",
"glue:getSchema",
"glue:getSchemaByDefinition",
"glue:getSchemaVersion",
"glue:getSchemaVersionsDiff",
"glue:getSession",
"glue:getStatement",
"glue:getTable",
"glue:getTables",
"glue:getTableVersions",
"glue:getTrigger",
"glue:getTriggers",
"glue:getUserDefinedFunction",
"glue:getUserDefinedFunctions",
"glue:getWorkflow",
"glue:getWorkflowRun",
"glue:getWorkflowRuns",
"glue:listCrawlers",
```

```
"glue:listCrawls",
"glue:listDataQualityResults",
"glue:listDataQualityRuleRecommendationRuns",
"glue:listDataQualityRulesetEvaluationRuns",
"glue:listDataQualityRulesets",
"glue:listDevEndpoints",
"glue:listMLTransforms",
"glue:listRegistries",
"glue:listSchemas",
"glue:listSchemaVersions",
"glue:listSessions",
"glue:listStatements",
"glue:querySchemaVersionMetadata",
"grafana:describeWorkspace",
"grafana:describeWorkspaceAuthentication",
"grafana:listPermissions",
"grafana:listVersions",
"grafana:listWorkspaces",
"greengrass:getConnectivityInfo",
"greengrass:getCoreDefinition",
"greengrass:getCoreDefinitionVersion",
"greengrass:getDeploymentStatus",
"greengrass:getDeviceDefinition",
"greengrass:getDeviceDefinitionVersion",
"greengrass:getFunctionDefinition",
"greengrass:getFunctionDefinitionVersion",
"greengrass:getGroup",
"greengrass:getGroupCertificateAuthority",
"greengrass:getGroupVersion",
"greengrass:getLoggerDefinition",
"greengrass:getLoggerDefinitionVersion",
"greengrass:getResourceDefinitionVersion",
"greengrass:getServiceRoleForAccount",
"greengrass:getSubscriptionDefinition",
"greengrass:getSubscriptionDefinitionVersion",
"greengrass:listCoreDefinitions",
"greengrass:listCoreDefinitionVersions",
"greengrass:listDeployments",
"greengrass:listDeviceDefinitions",
"greengrass:listDeviceDefinitionVersions",
"greengrass:listFunctionDefinitions",
"greengrass:listFunctionDefinitionVersions",
"greengrass:listGroups",
"greengrass:listGroupVersions",
```

```
"greengrass:listLoggerDefinitions",
"greengrass:listLoggerDefinitionVersions",
"greengrass:listResourceDefinitions",
"greengrass:listResourceDefinitionVersions",
"greengrass:listSubscriptionDefinitions",
"greengrass:listSubscriptionDefinitionVersions",
"guardduty: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:getWorkflow",
"imagebuilder:getWorkflowExecution",
"imagebuilder:getWorkflowStepExecution",
"imagebuilder:listComponentBuildVersions",
"imagebuilder:listComponents",
"imagebuilder:listContainerRecipes",
"imagebuilder:listDistributionConfigurations",
"imagebuilder:listImageBuildVersions",
"imagebuilder:listImagePipelineImages",
"imagebuilder:listImagePipelines",
"imagebuilder:listImageRecipes",
"imagebuilder:listImages",
"imagebuilder:listImageScanFindingAggregations",
"imagebuilder:listInfrastructureConfigurations",
"imagebuilder:listLifecycleExecutions",
"imagebuilder:listLifecycleExecutionResources",
"imagebuilder:listLifecyclePolicies",
"imagebuilder:listWorkflowBuildVersions",
"imagebuilder:listWorkflowExecutions",
"imagebuilder:listWorkflows",
"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:listCisScanConfigurations",
"inspector2:listCisScanResultsAggregatedByChecks",
"inspector2:listCisScanResultsAggregatedByTargetResource",
"inspector2:listCisScans",
"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:describeClusterOperationV2",
"kafka:describeClusterV2",
"kafka:describeConfiguration",
"kafka:describeConfigurationRevision",
"kafka:describeReplicator",
"kafka:describeVpcConnection",
"kafka:getBootstrapBrokers",
"kafka:getClusterPolicy",
"kafka:listConfigurations",
"kafka:listConfigurationRevisions",
"kafka:listClientVpcConnections",
"kafka:listClusterOperations",
"kafka:listClusterOperationsV2",
"kafka:listClusters",
"kafka:listClustersV2",
"kafka:listNodes",
"kafka:listReplicators",
"kafka:listScramSecrets",
"kafka:listVpcConnections",
"kafkaconnect:describeConnector",
"kafkaconnect:describeCustomPlugin",
```

```
"kafkaconnect:describeWorkerConfiguration",
"kafkaconnect:listConnectors",
"kafkaconnect:listCustomPlugins",
"kafkaconnect:listWorkerConfigurations",
"kendra:describeDataSource",
"kendra:describeFaq",
"kendra:describeIndex",
"kendra:listDataSources",
"kendra:listFaqs",
"kendra:listIndices",
"kinesis:describeStream",
"kinesis:describeStreamConsumer",
"kinesis:describeStreamSummary",
"kinesis:listShards",
"kinesis: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:getLogAnomalyDetector",
"logs:getLogDelivery",
"logs:getLogGroupFields",
"logs:listAnomalies",
"logs:listLogAnomalyDetectors",
"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",
"networkmonitor:getMonitor",
"networkmonitor:getProbe",
"networkmonitor:listMonitors",
"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",
"qbusiness:getApplication",
"qbusiness:getDataSource",
"qbusiness:getIndex",
"qbusiness:getRetriever",
"qbusiness:getWebExperience",
"qbusiness:listApplications",
"qbusiness:listDataSources",
"qbusiness:listDataSourceSyncJobs",
"qbusiness:listIndices",
"qbusiness:listRetrievers",
"qbusiness:listWebExperiences",
"quicksight:describeAccountCustomization",
"quicksight:describeAccountSettings",
"quicksight:describeAccountSubscription",
"quicksight:describeAnalysis",
"quicksight:describeAnalysisPermissions",
"quicksight:describeDashboard",
"quicksight:describeDashboardPermissions",
"quicksight:describeDataSet",
"quicksight:describeDataSetPermissions",
"quicksight:describeDataSetRefreshProperties",
"quicksight:describeDataSource",
"quicksight:describeDataSourcePermissions",
"quicksight:describeFolder",
"quicksight:describeFolderPermissions",
"quicksight:describeFolderResolvedPermissions",
"quicksight:describeGroup",
"quicksight:describeGroupMembership",
"quicksight:describeIAMPolicyAssignment",
"quicksight:describeIngestion",
"quicksight:describeIpRestriction",
"quicksight:describeNamespace",
"quicksight:describeRefreshSchedule",
"quicksight:describeTemplate",
"quicksight:describeTemplateAlias",
```

```
"quicksight:describeTemplatePermissions",
"quicksight:describeTheme",
"quicksight:describeThemeAlias",
"quicksight:describeThemePermissions",
"quicksight:describeTopic",
"quicksight:describeTopicPermissions",
"quicksight:describeTopicRefresh",
"quicksight:describeTopicRefreshSchedule",
"quicksight:describeUser",
"quicksight:describeVPCCConnection",
"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:listVPCCConnections",
"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:getBucketPolicy",
"s3express:listAllMyDirectoryBuckets",
"sagemaker:describeAction",
"sagemaker:describeAlgorithm",
"sagemaker:describeApp",
"sagemaker:describeAppImageConfig",
"sagemaker:describeArtifact",
"sagemaker:describeAutoMLJob",
"sagemaker:describeCluster",
"sagemaker:describeClusterNode",
"sagemaker:describeCodeRepository",
```

```
"sagemaker:describeCompilationJob",
"sagemaker:describeContext",
"sagemaker:describeDataQualityJobDefinition",
"sagemaker:describeDevice",
"sagemaker:describeDeviceFleet",
"sagemaker:describeDomain",
"sagemaker:describeEdgeDeploymentPlan",
"sagemaker:describeEdgePackagingJob",
"sagemaker:describeEndpoint",
"sagemaker:describeEndpointConfig",
"sagemaker:describeExperiment",
"sagemaker:describeFeatureGroup",
"sagemaker:describeFeatureMetadata",
"sagemaker:describeFlowDefinition",
"sagemaker:describeHub",
"sagemaker:describeHubContent",
"sagemaker:describeHumanTaskUi",
"sagemaker:describeHyperParameterTuningJob",
"sagemaker:describeImage",
"sagemaker:describeImageVersion",
"sagemaker:describeInferenceComponent",
"sagemaker:describeInferenceExperiment",
"sagemaker:describeInferenceRecommendationsJob",
"sagemaker:describeLabelingJob",
"sagemaker:describeModel",
"sagemaker:describeModelBiasJobDefinition",
"sagemaker:describeModelCard",
"sagemaker:describeModelCardExportJob",
"sagemaker:describeModelExplainabilityJobDefinition",
"sagemaker:describeModelPackage",
"sagemaker:describeModelPackageGroup",
"sagemaker:describeModelQualityJobDefinition",
"sagemaker:describeMonitoringSchedule",
"sagemaker:describeNotebookInstance",
"sagemaker:describeNotebookInstanceLifecycleConfig",
"sagemaker:describePipeline",
"sagemaker:describePipelineDefinitionForExecution",
"sagemaker:describePipelineExecution",
"sagemaker:describeProcessingJob",
"sagemaker:describeProject",
"sagemaker:describeSpace",
"sagemaker:describeStudioLifecycleConfig",
"sagemaker:describeSubscribedWorkteam",
"sagemaker:describeTrainingJob",
```

```
"sagemaker:describeTransformJob",
"sagemaker:describeTrial",
"sagemaker:describeTrialComponent",
"sagemaker:describeUserProfile",
"sagemaker:describeWorkforce",
"sagemaker:describeWorkteam",
"sagemaker:getDeviceFleetReport",
"sagemaker:getModelPackageGroupPolicy",
"sagemaker:getSagemakerServicecatalogPortfolioStatus",
"sagemaker:listActions",
"sagemaker:listAlgorithms",
"sagemaker:listAliases",
"sagemaker:listAppImageConfigs",
"sagemaker:listApps",
"sagemaker:listArtifacts",
"sagemaker:listAssociations",
"sagemaker:listAutoMLJobs",
"sagemaker:listCandidatesForAutoMLJob",
"sagemaker:listClusterNodes",
"sagemaker:listClusters",
"sagemaker:listCodeRepositories",
"sagemaker:listCompilationJobs",
"sagemaker:listContexts",
"sagemaker:listDataQualityJobDefinitions",
"sagemaker:listDeviceFleets",
"sagemaker:listDevices",
"sagemaker:listDomains",
"sagemaker:listEdgeDeploymentPlans",
"sagemaker:listEdgePackagingJobs",
"sagemaker:listEndpointConfigs",
"sagemaker:listEndpoints",
"sagemaker:listExperiments",
"sagemaker:listFeatureGroups",
"sagemaker:listFlowDefinitions",
"sagemaker:listHubContents",
"sagemaker:listHubContentVersions",
"sagemaker:listHubs",
"sagemaker:listHumanTaskUis",
"sagemaker:listHyperParameterTuningJobs",
"sagemaker:listImages",
"sagemaker:listImageVersions",
"sagemaker:listInferenceComponents",
"sagemaker:listInferenceExperiments",
"sagemaker:listInferenceRecommendationsJobs",
```



```
"sagemaker:listInferenceRecommendationsJobSteps",
"sagemaker:listLabelingJobs",
"sagemaker:listLabelingJobsForWorkteam",
"sagemaker:listLineageGroups",
"sagemaker:listModelBiasJobDefinitions",
"sagemaker:listModelCardExportJobs",
"sagemaker:listModelCards",
"sagemaker:listModelCardVersions",
"sagemaker:listModelExplainabilityJobDefinitions",
"sagemaker:listModelMetadata",
"sagemaker:listModelPackageGroups",
"sagemaker:listModelPackages",
"sagemaker:listModelQualityJobDefinitions",
"sagemaker:listModels",
"sagemaker:listMonitoringAlertHistory",
"sagemaker:listMonitoringAlerts",
"sagemaker:listMonitoringExecutions",
"sagemaker:listMonitoringSchedules",
"sagemaker:listNotebookInstanceLifecycleConfigs",
"sagemaker:listNotebookInstances",
"sagemaker:listPipelineExecutions",
"sagemaker:listPipelineExecutionSteps",
"sagemaker:listPipelineParametersForExecution",
"sagemaker:listPipelines",
"sagemaker:listProcessingJobs",
"sagemaker:listProjects",
"sagemaker:listSpaces",
"sagemaker:listStageDevices",
"sagemaker:listStudioLifecycleConfigs",
"sagemaker:listSubscribedWorkteams",
"sagemaker:listTags",
"sagemaker:listTrainingJobs",
"sagemaker:listTrainingJobsForHyperParameterTuningJob",
"sagemaker:listTransformJobs",
"sagemaker:listTrialComponents",
"sagemaker:listTrials",
"sagemaker:listUserProfiles",
"sagemaker:listWorkforces",
"sagemaker:listWorkteams",
"savingsplans:describeSavingsPlans",
"scheduler:getSchedule",
"scheduler:getScheduleGroup",
"scheduler:listScheduleGroups",
"scheduler:listSchedules",
```

```
"schemas:describeCodeBinding",
"schemas:describeDiscoverer",
"schemas:describeRegistry",
"schemas:describeSchema",
"schemas:getCodeBindingSource",
"schemas:getDiscoveredSchema",
"schemas:getResourcePolicy",
"schemas:listDiscoverers",
"schemas:listRegistries",
"schemas:listSchemas",
"schemas:listSchemaVersions",
"sdb:domainMetadata",
"sdb:listDomains",
"secretsmanager:describeSecret",
"secretsmanager:getResourcePolicy",
"secretsmanager:listSecrets",
"secretsmanager:listSecretVersionIds",
"securityhub:getEnabledStandards",
"securityhub:getFindings",
"securityhub:getInsightResults",
"securityhub:getInsights",
"securityhub:getMasterAccount",
"securityhub:getMembers",
"securityhub:listEnabledProductsForImport",
"securityhub:listInvitations",
"securityhub:listMembers",
"securitylake:getDataLakeExceptionSubscription",
"securitylake:getDataLakeOrganizationConfiguration",
"securitylake:getDataLakeSources",
"securitylake:getSubscriber",
"securitylake:listDataLakeExceptions",
"securitylake:listDataLakes",
"securitylake:listLogSources",
"securitylake:listSubscribers",
"serverlessrepo:getApplication",
"serverlessrepo:getApplicationPolicy",
"serverlessrepo:getCloudFormationTemplate",
"serverlessrepo:listApplicationDependencies",
"serverlessrepo:listApplications",
"serverlessrepo:listApplicationVersions",
"servicecatalog:describeConstraint",
"servicecatalog:describePortfolio",
"servicecatalog:describeProduct",
"servicecatalog:describeProductAsAdmin",
```

```
"servicecatalog:describeProductView",
"servicecatalog:describeProvisioningArtifact",
"servicecatalog:describeProvisioningParameters",
"servicecatalog:describeRecord",
"servicecatalog:listAcceptedPortfolioShares",
"servicecatalog:listConstraintsForPortfolio",
"servicecatalog:listLaunchPaths",
"servicecatalog:listPortfolioAccess",
"servicecatalog:listPortfolios",
"servicecatalog:listPortfoliosForProduct",
"servicecatalog:listPrincipalsForPortfolio",
"servicecatalog:listProvisioningArtifacts",
"servicecatalog:listRecordHistory",
"servicecatalog:scanProvisionedProducts",
"servicecatalog:searchProducts",
"servicequotas:getAssociationForServiceQuotaTemplate",
"servicequotas:getAWSDefaultServiceQuota",
"servicequotas:getRequestedServiceQuotaChange",
"servicequotas:getServiceQuota",
"servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:listAWSDefaultServiceQuotas",
"servicequotas:listRequestedServiceQuotaChangeHistory",
"servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:listServiceQuotas",
"servicequotas:listServices",
"ses:describeActiveReceiptRuleSet",
"ses:describeConfigurationSet",
"ses:describeReceiptRule",
"ses:describeReceiptRuleSet",
"ses:getAccount",
"ses:getAccountSendingEnabled",
"ses:getBlacklistReports",
"ses:getConfigurationSet",
"ses:getConfigurationSetEventDestinations",
"ses:getContactList",
"ses:getDedicatedIp",
"ses:getDedicatedIpPool",
"ses:getDedicatedIps",
"ses:getDeliverabilityDashboardOptions",
"ses:getDeliverabilityTestReport",
"ses:getDomainDeliverabilityCampaign",
"ses:getDomainStatisticsReport",
"ses:getEmailIdentity",
```

```
"ses:getIdentityDkimAttributes",
"ses:getIdentityMailFromDomainAttributes",
"ses:getIdentityNotificationAttributes",
"ses:getIdentityPolicies",
"ses:getIdentityVerificationAttributes",
"ses:getImportJob",
"ses:getSendQuota",
"ses:getSendStatistics",
"ses:listConfigurationSets",
"ses:listContactLists",
"ses:listContacts",
"ses:listCustomVerificationEmailTemplates",
"ses:listDedicatedIpPools",
"ses:listDeliverabilityTestReports",
"ses:listDomainDeliverabilityCampaigns",
"ses:listEmailIdentities",
"ses:listEmailTemplates",
"ses:listIdentities",
"ses:listIdentityPolicies",
"ses:listImportJobs",
"ses:listReceiptFilters",
"ses:listReceiptRuleSets",
"ses:listRecommendations",
"ses:listTagsForResource",
"ses:listTemplates",
"ses:listVerifiedEmailAddresses",
"shield:describeAttack",
"shield:describeProtection",
"shield:describeSubscription",
"shield:listAttacks",
"shield:listProtections",
"sms-voice:getConfigurationSetEventDestinations",
"sms:getConnectors",
"sms:getReplicationJobs",
"sms:getReplicationRuns",
"sms:getServers",
"snowball:describeAddress",
"snowball:describeAddresses",
"snowball:describeJob",
"snowball:getSnowballUsage",
"snowball:listJobs",
"snowball:listServiceVersions",
"sns:checkIfPhoneNumberIsOptedOut",
"sns:getDataProtectionPolicy",
```

```
"sns:getEndpointAttributes",
"sns:getPlatformApplicationAttributes",
"sns:getSMSAttributes",
"sns:getSMSSandboxAccountStatus",
"sns:getSubscriptionAttributes",
"sns:getTopicAttributes",
"sns:listEndpointsByPlatformApplication",
"sns:listOriginationNumbers",
"sns:listPhoneNumbersOptedOut",
"sns:listPlatformApplications",
"sns:listSMSSandboxPhoneNumbers",
"sns:listSubscriptions",
"sns:listSubscriptionsByTopic",
"sns:listTopics",
"sqs:getQueueAttributes",
"sqs:getQueueUrl",
"sqs:listDeadLetterSourceQueues",
"sqs:listQueues",
"ssm-contacts:describeEngagement",
"ssm-contacts:describePage",
"ssm-contacts:getContact",
"ssm-contacts:getContactChannel",
"ssm-contacts:getContactPolicy",
"ssm-contacts:getRotation",
"ssm-contacts:getRotationOverride",
"ssm-contacts:listContactChannels",
"ssm-contacts:listContacts",
"ssm-contacts:listEngagements",
"ssm-contacts:listPageReceipts",
"ssm-contacts:listPageResolutions",
"ssm-contacts:listPagesByContact",
"ssm-contacts:listPagesByEngagement",
"ssm-contacts:listPreviewRotationShifts",
"ssm-contacts:listRotationOverrides",
"ssm-contacts:listRotations",
"ssm-contacts:listRotationShifts",
"ssm-incidents:getIncidentRecord",
"ssm-incidents:getReplicationSet",
"ssm-incidents:getResourcePolicies",
"ssm-incidents:getResponsePlan",
"ssm-incidents:getTimelineEvent",
"ssm-incidents:listIncidentRecords",
"ssm-incidents:listRelatedItems",
"ssm-incidents:listReplicationSets",
```

```
"ssm-incidents:listResponsePlans",
"ssm-incidents:listTimelineEvents",
"ssm-sap:getApplication",
"ssm-sap:getComponent",
"ssm-sap:getDatabase",
"ssm-sap:getOperation",
"ssm-sap:getResourcePermission",
"ssm-sap:listApplications",
"ssm-sap:listComponents",
"ssm-sap:listDatabases",
"ssm-sap:listOperations",
"ssm:describeActivations",
"ssm:describeAssociation",
"ssm:describeAssociationExecutions",
"ssm:describeAssociationExecutionTargets",
"ssm:describeAutomationExecutions",
"ssm:describeAutomationStepExecutions",
"ssm:describeAvailablePatches",
"ssm:describeDocument",
"ssm:describeDocumentPermission",
"ssm:describeEffectiveInstanceAssociations",
"ssm:describeEffectivePatchesForPatchBaseline",
"ssm:describeInstanceAssociationsStatus",
"ssm:describeInstanceInformation",
"ssm:describeInstancePatches",
"ssm:describeInstancePatchStates",
"ssm:describeInstancePatchStatesForPatchGroup",
"ssm:describeInventoryDeletions",
"ssm:describeMaintenanceWindowExecutions",
"ssm:describeMaintenanceWindowExecutionTaskInvocations",
"ssm:describeMaintenanceWindowExecutionTasks",
"ssm:describeMaintenanceWindows",
"ssm:describeMaintenanceWindowSchedule",
"ssm:describeMaintenanceWindowsForTarget",
"ssm:describeMaintenanceWindowTargets",
"ssm:describeMaintenanceWindowTasks",
"ssm:describeOpsItems",
"ssm:describeParameters",
"ssm:describePatchBaselines",
"ssm:describePatchGroups",
"ssm:describePatchGroupState",
"ssm:describePatchProperties",
"ssm:describeSessions",
"ssm:getAutomationExecution",
```

```
"ssm:getCalendarState",
"ssm:getCommandInvocation",
"ssm:getConnectionStatus",
"ssm:getDefaultPatchBaseline",
"ssm:getDeployablePatchSnapshotForInstance",
"ssm:getInventorySchema",
"ssm:getMaintenanceWindow",
"ssm:getMaintenanceWindowExecution",
"ssm:getMaintenanceWindowExecutionTask",
"ssm:getMaintenanceWindowExecutionTaskInvocation",
"ssm:getMaintenanceWindowTask",
"ssm:getOpsItem",
"ssm:getOpsMetadata",
"ssm:getOpsSummary",
"ssm:getPatchBaseline",
"ssm:getPatchBaselineForPatchGroup",
"ssm:getResourcePolicies",
"ssm:getServiceSetting",
"ssm:listAssociations",
"ssm:listAssociationVersions",
"ssm:listCommandInvocations",
"ssm:listCommands",
"ssm:listComplianceItems",
"ssm:listComplianceSummaries",
"ssm:listDocuments",
"ssm:listDocumentMetadataHistory",
"ssm:listDocumentVersions",
"ssm:listOpsItemEvents",
"ssm:listOpsItemRelatedItems",
"ssm:listOpsMetadata",
"ssm:listResourceComplianceSummaries",
"ssm:listResourceDataSync",
"ssm:listTagsForResource",
"sso:describeApplicationAssignment",
"sso:describeApplicationProvider",
"sso:describeApplication",
"sso:describeInstance",
"sso:describeTrustedTokenIssuer",
"sso:getApplicationAccessScope",
"sso:getApplicationAssignmentConfiguration",
"sso:getApplicationAuthenticationMethod",
"sso:getApplicationGrant",
"sso:getApplicationInstance",
"sso:getApplicationTemplate",
```

```
"sso:getManagedApplicationInstance",
"sso:getSharedSsoConfiguration",
"sso:listApplicationAccessScopes",
"sso:listApplicationAssignments",
"sso:listApplicationAuthenticationMethods",
"sso:listApplicationGrants",
"sso:listApplicationInstances",
"sso:listApplicationProviders",
"sso:listApplications",
"sso:listApplicationTemplates",
"sso:listDirectoryAssociations",
"sso:listInstances",
"sso:listProfileAssociations",
"sso:listTrustedTokenIssuers",
"states:describeActivity",
"states:describeExecution",
"states:describeMapRun",
"states:describeStateMachine",
"states:describeStateMachineAlias",
"states:describeStateMachineForExecution",
"states:getExecutionHistory",
"states:listActivities",
"states:listExecutions",
"states:listMapRuns",
"states:listStateMachineAliases",
"states:listStateMachines",
"states:listStateMachineVersions",
"storagegateway:describeBandwidthRateLimit",
"storagegateway:describeCache",
"storagegateway:describeCachediSCSIVolumes",
"storagegateway:describeFileSystemAssociations",
"storagegateway:describeGatewayInformation",
"storagegateway:describeMaintenanceStartTime",
"storagegateway:describeNFSFileShares",
"storagegateway:describeSMBFileShares",
"storagegateway:describeSMBSettings",
"storagegateway:describeSnapshotSchedule",
"storagegateway:describeStorediSCSIVolumes",
"storagegateway:describeTapeArchives",
"storagegateway:describeTapeRecoveryPoints",
"storagegateway:describeTapes",
"storagegateway:describeUploadBuffer",
"storagegateway:describeVTLDevices",
"storagegateway:describeWorkingStorage",
```



```
"storagegateway:listAutomaticTapeCreationPolicies",
"storagegateway:listFileShares",
"storagegateway:listFileSystemAssociations",
"storagegateway:listGateways",
"storagegateway:listLocalDisks",
"storagegateway:listTagsForResource",
"storagegateway:listTapes",
"storagegateway:listVolumeInitiators",
"storagegateway:listVolumeRecoveryPoints",
"storagegateway:listVolumes",
"swf:countClosedWorkflowExecutions",
"swf:countOpenWorkflowExecutions",
"swf:countPendingActivityTasks",
"swf:countPendingDecisionTasks",
"swf:describeActivityType",
"swf:describeDomain",
"swf:describeWorkflowExecution",
"swf:describeWorkflowType",
"swf:getWorkflowExecutionHistory",
"swf:listActivityTypes",
"swf:listClosedWorkflowExecutions",
"swf:listDomains",
"swf:listOpenWorkflowExecutions",
"swf:listWorkflowTypes",
"synthetics:describeCanaries",
"synthetics:describeCanariesLastRun",
"synthetics:describeRuntimeVersions",
"synthetics:getCanary",
"synthetics:getCanaryRuns",
"synthetics:getGroup",
"synthetics:listAssociatedGroups",
"synthetics:listGroupResources",
"synthetics:listGroups",
"tiros:createQuery",
"tiros:getQueryAnswer",
"tiros:getQueryExplanation",
"transcribe:describeLanguageModel",
"transcribe:getCallAnalyticsCategory",
"transcribe:getCallAnalyticsJob",
"transcribe:getMedicalTranscriptionJob",
"transcribe:getMedicalVocabulary",
"transcribe:getTranscriptionJob",
"transcribe:getVocabulary",
"transcribe:getVocabularyFilter",
```

```
"transcribe:listCallAnalyticsCategories",
"transcribe:listCallAnalyticsJobs",
"transcribe:listLanguageModels",
"transcribe:listMedicalTranscriptionJobs",
"transcribe:listMedicalVocabularies",
"transcribe:listTranscriptionJobs",
"transcribe:listVocabularies",
"transcribe:listVocabularyFilters",
"transfer:describeAccess",
"transfer:describeAgreement",
"transfer:describeConnector",
"transfer:describeExecution",
"transfer:describeProfile",
"transfer:describeServer",
"transfer:describeUser",
"transfer:describeWorkflow",
"transfer:listAccesses",
"transfer:listAgreements",
"transfer:listConnectors",
"transfer:listExecutions",
"transfer:listHostKeys",
"transfer:listProfiles",
"transfer:listServers",
"transfer:listTagsForResource",
"transfer:listUsers",
"transfer:listWorkflows",
"transfer:sendWorkflowStepState",
"trustedadvisor:getOrganizationRecommendation",
"trustedadvisor:getRecommendation",
"trustedadvisor:listChecks",
"trustedadvisor:listOrganizationRecommendationAccounts",
"trustedadvisor:listOrganizationRecommendationResources",
"trustedadvisor:listOrganizationRecommendations",
"trustedadvisor:listRecommendationResources",
"trustedadvisor:listRecommendations",
"verifiedpermissions:getIdentitySource",
"verifiedpermissions:getPolicy",
"verifiedpermissions:getPolicyStore",
"verifiedpermissions:getPolicyTemplate",
"verifiedpermissions:getSchema",
"verifiedpermissions:listIdentitySources",
"verifiedpermissions:listPolicies",
"verifiedpermissions:listPolicyStores",
"verifiedpermissions:listPolicyTemplates",
```

```
"vpc-lattice:getAccessLogSubscription",
"vpc-lattice:getAuthPolicy",
"vpc-lattice:getListener",
"vpc-lattice:getResourcePolicy",
"vpc-lattice:getRule",
"vpc-lattice:getService",
"vpc-lattice:getServiceNetwork",
"vpc-lattice:getServiceNetworkServiceAssociation",
"vpc-lattice:getServiceNetworkVpcAssociation",
"vpc-lattice:getTargetGroup",
"vpc-lattice:listAccessLogSubscriptions",
"vpc-lattice:listListeners",
"vpc-lattice:listRules",
"vpc-lattice:listServiceNetworks",
"vpc-lattice:listServiceNetworkServiceAssociations",
"vpc-lattice:listServiceNetworkVpcAssociations",
"vpc-lattice:listServices",
"vpc-lattice:listTargetGroups",
"vpc-lattice:listTargets",
"waf-regional:getByteMatchSet",
"waf-regional:getChangeTokenStatus",
"waf-regional:getGeoMatchSet",
"waf-regional:getIPSet",
"waf-regional:getLoggingConfiguration",
"waf-regional:getRateBasedRule",
"waf-regional:getRegexMatchSet",
"waf-regional:getRegexPatternSet",
"waf-regional:getRule",
"waf-regional:getRuleGroup",
"waf-regional:getSqlInjectionMatchSet",
"waf-regional:getWebACL",
"waf-regional:getWebACLForResource",
"waf-regional:listActivatedRulesInRuleGroup",
"waf-regional:listByteMatchSets",
"waf-regional:listGeoMatchSets",
"waf-regional:listIPSets",
"waf-regional:listLoggingConfigurations",
"waf-regional:listRateBasedRules",
"waf-regional:listRegexMatchSets",
"waf-regional:listRegexPatternSets",
"waf-regional:listResourcesForWebACL",
"waf-regional:listRuleGroups",
"waf-regional:listRules",
"waf-regional:listSqlInjectionMatchSets",
```

```
"waf-regional:listWebACLs",
"waf:getByteMatchSet",
"waf:getChangeTokenStatus",
"waf:getGeoMatchSet",
"waf:getIPSet",
"waf:getLoggingConfiguration",
"waf:getRateBasedRule",
"waf:getRegexMatchSet",
"waf:getRegexPatternSet",
"waf:getRule",
"waf:getRuleGroup",
"waf:getSampledRequests",
"waf:getSizeConstraintSet",
"waf:getSqlInjectionMatchSet",
"waf:getWebACL",
"waf:getXssMatchSet",
"waf:listActivatedRulesInRuleGroup",
"waf:listByteMatchSets",
"waf:listGeoMatchSets",
"waf:listIPSets",
"waf:listLoggingConfigurations",
"waf:listRateBasedRules",
"waf:listRegexMatchSets",
"waf:listRegexPatternSets",
"waf:listRuleGroups",
"waf:listRules",
"waf:listSizeConstraintSets",
"waf:listSqlInjectionMatchSets",
"waf:listWebACLs",
"waf:listXssMatchSets",
"wafv2:checkCapacity",
"wafv2:describeManagedRuleGroup",
"wafv2:getIPSet",
"wafv2:getLoggingConfiguration",
"wafv2:getPermissionPolicy",
"wafv2:getRateBasedStatementManagedKeys",
"wafv2:getRegexPatternSet",
"wafv2:getRuleGroup",
"wafv2:getSampledRequests",
"wafv2:getWebACL",
"wafv2:getWebACLForResource",
"wafv2:listAvailableManagedRuleGroups",
"wafv2:listIPSets",
"wafv2:listLoggingConfigurations",
```

```
"wafv2:listRegexPatternSets",
"wafv2:listResourcesForWebACL",
"wafv2:listRuleGroups",
"wafv2:listTagsForResource",
"wafv2:listWebACLs",
"workdocs:checkAlias",
"workdocs:describeAvailableDirectories",
"workdocs:describeInstances",
"workmail:describeGroup",
"workmail:describeOrganization",
"workmail:describeResource",
"workmail:describeUser",
"workmail:listAliases",
"workmail:listGroupMembers",
"workmail:listGroups",
"workmail:listMailboxPermissions",
"workmail:listOrganizations",
"workmail:listResourceDelegates",
"workmail:listResources",
"workmail:listUsers",
"workspaces-web:getBrowserSettings",
"workspaces-web:getIdentityProvider",
"workspaces-web:getNetworkSettings",
"workspaces-web:getPortal",
"workspaces-web:getPortalServiceProviderMetadata",
"workspaces-web:getTrustStoreCertificate",
"workspaces-web:getUserSettings",
"workspaces-web:listBrowserSettings",
"workspaces-web:listIdentityProviders",
"workspaces-web:listNetworkSettings",
"workspaces-web:listPortals",
"workspaces-web:listTagsForResource",
"workspaces-web:listTrustStoreCertificates",
"workspaces-web:listTrustStores",
"workspaces-web:listUserSettings",
"workspaces:describeAccount",
"workspaces:describeAccountModifications",
"workspaces:describeIpGroups",
"workspaces:describeTags",
"workspaces:describeWorkspaceBundles",
"workspaces:describeWorkspaceDirectories",
"workspaces:describeWorkspaceImages",
"workspaces:describeWorkspaces",
"workspaces:describeWorkspacesConnectionStatus",
```

```
        "xray:getEncryptionConfig",
        "xray:getGroup",
        "xray:getGroups",
        "xray:getSamplingRules",
        "xray:listResourcePolicies"
    ],
    "Effect" : "Allow",
    "Resource" : [
        "*"
    ]
}
],
"Version" : "2012-10-17"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSystemsManagerAccountDiscoveryServicePolicy

Descrizione: concede a AWS Systems Manager (SSM) l'autorizzazione a scoprire Account AWS informazioni.

AWSSystemsManagerAccountDiscoveryServicePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 ottobre 2019, 17:21 UTC
- Ora modificata: 17 ottobre 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSystemsManagerChangeManagementServicePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate dal framework di gestione delle modifiche di AWS Systems Manager.

AWSSystemsManagerChangeManagementServicePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 07 dicembre 2020, 22:21 UTC
- Ora modificata: 07 dicembre 2020, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSystemsManagerForSAPFullAccess

Descrizione: Fornisce l'accesso completo al servizio AWS Systems Manager for SAP

AWSSystemsManagerForSAPFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSystemsManagerForSAPFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2022, 02:11 UTC
- Ora modificata: 18 novembre 2022, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSystemsManagerForSAPReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio AWS Systems Manager for SAP

AWSSystemsManagerForSAPReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSSystemsManagerForSAPReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2022, 02:11 UTC
- Ora modificata: 17 novembre 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",

```

```
    "ssm-sap:list*"
  ],
  "Resource" : "arn:*:ssm-sap:*:*:*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Descrizione: ruolo IAM per SSM Explorer per la gestione delle operazioni OpsData correlate

AWSSystemsManagerOpsDataSyncServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 aprile 2021, 20:42 UTC
- Ora modificata: 28 giugno 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSThinkboxAssetServerPolicy

Descrizione: questa politica concede a AWS Portal Asset Server le autorizzazioni necessarie per il normale funzionamento.

AWSThinkboxAssetServerPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSThinkboxAssetServerPolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:18 UTC
- Ora modificata: 27 maggio 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSThinkboxAWSPortalAdminPolicy

Descrizione: questa politica garantisce al software Deadline di AWS Thinkbox l'accesso completo a più AWS servizi, come richiesto per l'amministrazione del portale. AWS Ciò include l'accesso per creare tag arbitrari su diversi tipi di risorse EC2.

AWSThinkboxAWSPortalAdminPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSThinkboxAWSPortalAdminPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:41 UTC
- Ora modificata: 12 aprile 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "AWSThinkboxAWSPortal7",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal8",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
```

```

        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
    ]
},
{
    "Sid" : "AWSThinkboxAWSPortal10",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetUser"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AWSThinkboxAWSPortal11",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetInstanceProfile"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:instance-profile/AWSPortal*"
    ]
},
{
    "Sid" : "AWSThinkboxAWSPortal12",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:policy/AWSPortal*"
    ]
},
{
    "Sid" : "AWSThinkboxAWSPortal13",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetRole",

```



```
    "iam:GetRolePolicy"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPortal*",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal14",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPortal*",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2fleet.amazonaws.com",
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal15",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "ec2fleet.amazonaws.com",
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com"
      ]
    }
  }
},
},
```

```

{
  "Sid" : "AWSThinkboxAWSPortal16",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketVersioning",
    "s3:PutBucketAcl",
    "s3:PutBucketCORS",
    "s3:PutBucketVersioning",
    "s3:GetBucketAcl",
    "s3:GetObject",
    "s3:PutBucketLogging",
    "s3:PutBucketTagging",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutEncryptionConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteBucketPolicy",
    "s3:DeleteObjectVersion"
  ],
  "Resource" : [
    "arn:aws:s3::*:awsportal*",
    "arn:aws:s3::*:stack*",
    "arn:aws:s3::*:aws-portal-cache*",
    "arn:aws:s3::*:logs-for-aws-portal-cache*",
    "arn:aws:s3::*:logs-for-stack*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal17",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketPolicy"
  ],
  "Resource" : [
    "arn:aws:s3::*:logs-for-aws-portal-cache*"
  ]
},
{

```

```

    "Sid" : "AWSThinkboxAWSPortal18",
    "Effect" : "Allow",
    "Action" : [
        "s3:PutBucketOwnershipControls"
    ],
    "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
    ]
},
{
    "Sid" : "AWSThinkboxAWSPortal19",
    "Effect" : "Allow",
    "Action" : [
        "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AWSThinkboxAWSPortal20",
    "Effect" : "Allow",
    "Action" : [
        "dynamodb:Scan"
    ],
    "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
},
{
    "Sid" : "AWSThinkboxAWSPortal21",
    "Effect" : "Allow",
    "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation>DeleteStack",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
    ],
    "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",

```

```
    "arn:aws:cloudformation:*:*:stack/Deadline*/*"
  ],
},
{
  "Sid" : "AWSThinkboxAWSPortal22",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:EstimateTemplateCost",
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal23",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:PutRetentionPolicy",
    "logs>DeleteRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
},
{
  "Sid" : "AWSThinkboxAWSPortal24",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups",
    "logs>CreateLogGroup"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal25",
  "Effect" : "Allow",
  "Action" : [
    "kms:Encrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
```

```

    "StringLike" : {
      "kms:ViaService" : [
        "s3.*.amazonaws.com",
        "secretsmanager.*.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal26",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "secretsmanager:Name" : [
          "rcs-tls-pw*"
        ]
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal27",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:DeleteSecret",
      "secretsmanager:UpdateSecret",
      "secretsmanager:DescribeSecret",
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSThinkboxAWSPortalGatewayPolicy

Descrizione: questo criterio concede al computer AWS Portal Gateway le autorizzazioni necessarie per il normale funzionamento.

AWSThinkboxAWSPortalGatewayPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSThinkboxAWSPortalGatewayPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:05 UTC
- Ora modificata: 30 giugno 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:rds-tls-pw-stack*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSThinkboxAWSPortalWorkerPolicy

Descrizione: questa politica concede a Deadline Workers in AWS Portal le autorizzazioni necessarie per il normale funzionamento.

AWSThinkboxAWSPortalWorkerPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSThinkboxAWSPortalWorkerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:15 UTC
- Ora modificata: 07 dicembre 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Descrizione: concede le autorizzazioni necessarie per il funzionamento del Deadline Resource AWS Tracker di Thinkbox. Ciò include l'accesso completo ad alcune azioni EC2, tra cui e. DeleteFleets CancelSpotFleetRequests

AWSThinkboxDeadlineResourceTrackerAccessPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSThinkboxDeadlineResourceTrackerAccessPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:25 UTC
- Ora modificata: 27 maggio 2020, 19:25 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Descrizione: concede le autorizzazioni necessarie per creare, distruggere e amministrare Deadline Resource Tracker di AWS Thinkbox.

AWSThinkboxDeadlineResourceTrackerAdminPolicy è [una politica gestita](#).AWS

Utilizzo di questa politica

Puoi collegarti AWSThinkboxDeadlineResourceTrackerAdminPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:29 UTC
- Ora modificata: 12 aprile 2024, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
```



```

    "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
  ],
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker4",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:CreateTable",
    "dynamodb>DeleteTable",
    "dynamodb:DescribeTable",
    "dynamodb:ListTagsOfResource",
    "dynamodb:TagResource",
    "dynamodb:UntagResource"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker5",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:BatchWriteItem",
    "dynamodb:Scan"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker6",
  "Effect" : "Allow",
  "Action" : [
    "events>DeleteRule",
    "events:DescribeRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
  ]
}

```

```
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker7",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/DeadlineResourceTracker*"
    ]
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker8",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetUser"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker9",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "dynamodb.application-autoscaling.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker10",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ]
  }
}
```

```

    ],
    "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "lambda.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AWSThinkboxDeadlineResourceTracker11",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "application-autoscaling.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AWSThinkboxDeadlineResourceTracker12",
    "Effect" : "Allow",
    "Action" : [
        "lambda:GetEventSourceMapping"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "AWSThinkboxDeadlineResourceTracker13",
    "Effect" : "Allow",
    "Action" : [

```

```

        "lambda:CreateEventSourceMapping",
        "lambda>DeleteEventSourceMapping"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringLike" : {
            "lambda:FunctionArn" : [
                "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
            ]
        }
    }
},
{
    "Sid" : "AWSThinkboxDeadlineResourceTracker14",
    "Effect" : "Allow",
    "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
    ],
    "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
    ],
    "Condition" : {
        "StringLike" : {
            "lambda:Principal" : "events.amazonaws.com"
        }
    }
},
{
    "Sid" : "AWSThinkboxDeadlineResourceTracker15",
    "Effect" : "Allow",
    "Action" : [
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda>DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",

```

```

    "lambda:UpdateFunctionConfiguration"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
  ]
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker16",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*/deadline_aws_resource_tracker-*.zip",
    "arn:aws:s3::*/DeadlineAWSResourceTrackerTemplate-*.yaml"
  ]
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker17",
  "Effect" : "Allow",
  "Action" : [
    "sqs:CreateQueue",
    "sqs>DeleteQueue",
    "sqs:GetQueueAttributes",
    "sqs:ListQueueTags",
    "sqs:TagQueue",
    "sqs:UntagQueue"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
    "arn:aws:sqs:*:*:DeadlineResourceTracker*"
  ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Descrizione: concede le autorizzazioni necessarie per il plug-in Deadline Spot Event di AWS Thinkbox. Ciò include l'autorizzazione a richiedere, modificare e annullare una flotta spot, nonché un'autorizzazione limitata. PassRole

AWSThinkboxDeadlineSpotEventPluginAdminPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSThinkboxDeadlineSpotEventPluginAdminPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:38 UTC
- Ora modificata: 27 maggio 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Descrizione: concedi le autorizzazioni necessarie per un'istanza EC2 che esegue il software AWS Thinkbox Deadline Spot Event Plugin Worker.

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSThinkboxDeadlineSpotEventPluginWorkerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:35 UTC
- Ora modificata: 07 dicembre 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSTransferConsoleFullAccess

Descrizione: fornisce l'accesso completo a AWS Transfer tramite AWS Management Console

AWSTransferConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSTransferConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 dicembre 2020, 19:33 UTC
- Ora modificata: 14 dicembre 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSTransferFullAccess

Descrizione: fornisce l'accesso completo al servizio di AWS trasferimento.

AWSTransferFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSTransferFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 dicembre 2020, 19:37 UTC
- Ora modificata: 14 dicembre 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSTransferLoggingAccess

Descrizione: consente a AWS Transfer l'accesso completo per creare flussi e gruppi di log e inserire eventi di registro nel tuo account

AWSTransferLoggingAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSTransferLoggingAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 gennaio 2019, 15:32 UTC
- Ora modificata: 14 gennaio 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSTransferReadOnlyAccess

Descrizione: Fornisci l'accesso in sola lettura ai servizi di AWS trasferimento.

AWSTransferReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSTransferReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 agosto 2020, 17:54 UTC
- Ora modificata: 27 agosto 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSTrustedAdvisorPriorityFullAccess

Descrizione: Fornisce l'accesso completo a AWS Trusted Advisor Priority. Questa politica consente inoltre all'utente di aggiungere Trusted Advisor come servizio affidabile con AWS Organizations e di specificare account amministrativi delegati per Trusted Advisor Priority.

AWSTrustedAdvisorPriorityFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSTrustedAdvisorPriorityFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 16 agosto 2022, 16:08 UTC
- Ora modificata: 16 agosto 2022, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Trusted Advisor Priority. Ciò include l'autorizzazione a visualizzare gli account degli amministratori delegati.

AWSTrustedAdvisorPriorityReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSTrustedAdvisorPriorityReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 16 agosto 2022, 16:35 UTC
- Ora modificata: 16 agosto 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
}
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSTrustedAdvisorReportingServiceRolePolicy

Descrizione: Politica di servizio per la reportistica su più account di Trusted Advisor

AWSTrustedAdvisorReportingServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 novembre 2019, 17:41 UTC

- Ora modificata: 28 febbraio 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSTrustedAdvisorServiceRolePolicy

Descrizione: Accesso al servizio AWS Trusted Advisor per ridurre i costi, aumentare le prestazioni e migliorare la sicurezza dell' AWS ambiente.

AWSTrustedAdvisorServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 22 febbraio 2018, 21:24 UTC
- Ora modificata: 11 giugno 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
```



```
"autoscaling:DescribeLaunchConfigurations",
"ce:GetReservationPurchaseRecommendation",
"ce:GetSavingsPlansPurchaseRecommendation",
"cloudformation:DescribeAccountLimits",
"cloudformation:DescribeStacks",
"cloudformation:ListStacks",
"cloudfront:ListDistributions",
"cloudtrail:DescribeTrails",
"cloudtrail:GetTrailStatus",
"cloudtrail:GetTrail",
"cloudtrail:ListTrails",
"cloudtrail:GetEventSelectors",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"dax:DescribeClusters",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"ec2:DescribeAddresses",
"ec2:DescribeReservedInstances",
"ec2:DescribeInstances",
"ec2:DescribeVpcs",
"ec2:DescribeInternetGateways",
"ec2:DescribeImages",
"ec2:DescribeNatGateways",
"ec2:DescribeVolumes",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeRegions",
"ec2:DescribeReservedInstancesOfferings",
"ec2:DescribeRouteTables",
"ec2:DescribeSnapshots",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DescribeLaunchTemplateVersions",
"ec2:GetManagedPrefixListEntries",
"ecs:DescribeTaskDefinition",
"ecs:ListTaskDefinitions",
"elasticloadbalancing:DescribeAccountLimits",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
```

```
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"iam:GenerateCredentialReport",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetServerCertificate",
"iam:ListServerCertificates",
"iam:ListSAMLProviders",
"kinesis:DescribeLimits",
"kafka:DescribeClusterV2",
"kafka:ListClustersV2",
"kafka:ListNodes",
"network-firewall:ListFirewalls",
"network-firewall:DescribeFirewall",
"outposts:ListAssets",
"outposts:GetOutpost",
"outposts:ListOutposts",
"rds:DescribeAccountAttributes",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEvents",
"rds:DescribeOptionGroupOptions",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribeReservedDBInstances",
"rds:DescribeReservedDBInstancesOfferings",
"rds:ListTagsForResource",
"redshift:DescribeClusters",
"redshift:DescribeReservedNodeOfferings",
"redshift:DescribeReservedNodes",
"route53:GetAccountLimit",
"route53:GetHealthCheck",
"route53:GetHostedZone",
"route53:ListHealthChecks",
"route53:ListHostedZones",
```

```
    "route53:ListHostedZonesByName",
    "route53:ListResourceRecordSets",
    "route53resolver:ListResolverEndpoints",
    "route53resolver:ListResolverEndpointIpAddresses",
    "s3:GetAccountPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketVersioning",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetLifecycleConfiguration",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "ses:GetSendQuota",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSUserNotificationsServiceLinkedRolePolicy

Descrizione: consente alle notifiche AWS utente di chiamare AWS i servizi per tuo conto.

AWSUserNotificationsServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 19 aprile 2023, 13:28 UTC
- Ora modificata: 19 aprile 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSVendorInsightsAssessorFullAccess

Descrizione: fornisce l'accesso completo alla visualizzazione delle risorse Vendor Insights autorizzate e alla gestione degli abbonamenti Vendor Insights

AWSVendorInsightsAssessorFullAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSVendorInsightsAssessorFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2022, 15:05 UTC
- Ora modificata: 01 dicembre 2022, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSVendorInsightsAssessorReadOnly

Descrizione: fornisce l'accesso in sola lettura per la visualizzazione delle risorse Vendor Insights autorizzate

AWSVendorInsightsAssessorReadOnly [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSVendorInsightsAssessorReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2022, 15:05 UTC
- Ora modificata: 01 dicembre 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSVendorInsightsVendorFullAccess

Descrizione: fornisce l'accesso completo per la creazione e la gestione delle risorse di Vendor Insights

AWSVendorInsightsVendorFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `AWSVendorInsightsVendorFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2022, 15:05 UTC
- Ora modificata: 19 ottobre 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"  
  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSVendorInsightsVendorReadOnly

Descrizione: fornisce l'accesso in sola lettura per la visualizzazione delle risorse di Vendor Insights

AWSVendorInsightsVendorReadOnly è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti AWSVendorInsightsVendorReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2022, 15:05 UTC
- Ora modificata: 01 dicembre 2022, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSVpcLatticeServiceRolePolicy

Descrizione: consente a VPC Lattice di accedere alle AWS risorse per tuo conto.

AWSVpcLatticeServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 30 novembre 2022, 20:47 UTC
- Ora modificata: 30 novembre 2022, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSVPCS2SVpnServiceRolePolicy

Descrizione: consenti alla VPN da sito a sito di creare e gestire risorse relative alle tue connessioni VPN.

AWSVPCS2SVpnServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 6 agosto 2019, 14:13 UTC
- Ora modificata: 6 agosto 2019, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSVPCTransitGatewayServiceRolePolicy

Descrizione: consenti a VPC Transit Gateway di creare e gestire le risorse necessarie per gli allegati VPC Transit Gateway.

AWSVPCTransitGatewayServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 novembre 2018, 16:21 UTC
- Ora modificata: 15 aprile 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : ""
    }
  ]
}
```



```
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSVPCVerifiedAccessServiceRolePolicy

Descrizione: politica per consentire al servizio AWS Verified Access di fornire gli endpoint per conto dell'utente

AWSVPCVerifiedAccessServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 29 novembre 2022, 03:35 UTC
- Ora modificata: 17 novembre 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSWAFConsoleFullAccess

Descrizione: Fornisce l'accesso completo a AWS WAF tramite AWS Management Console. Tieni presente che questa politica concede anche le autorizzazioni per elencare e aggiornare le CloudFront distribuzioni Amazon, le autorizzazioni per visualizzare i sistemi di bilanciamento del carico su Elastic Load AWS Balancing, le autorizzazioni per visualizzare le API e le fasi REST di Amazon API Gateway, le autorizzazioni per elencare e visualizzare i parametri Amazon e le autorizzazioni per visualizzare le regioni abilitate all' CloudWatch interno dell'account.

AWSWAFConsoleFullAccess è una [politica](#) gestita AWS.

Utilizzo di questa politica

Puoi collegarti `AWSWAFConsoleFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 aprile 2020, 18:38 UTC
- Ora modificata: 05 giugno 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSWAFConsoleReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS WAF tramite AWS Management Console. Tieni presente che questa politica concede anche le autorizzazioni per elencare le CloudFront distribuzioni Amazon, le autorizzazioni per visualizzare i sistemi di bilanciamento del carico su Elastic Load AWS Balancing, le autorizzazioni per visualizzare le API e le fasi REST di Amazon API Gateway, le autorizzazioni per elencare e visualizzare i parametri Amazon e le autorizzazioni per visualizzare le regioni abilitate all' CloudWatch interno dell'account.

AWSWAFConsoleReadOnlyAccess è una [politica](#) gestita AWS.

Utilizzo di questa politica

Puoi collegarti AWSWAFConsoleReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 aprile 2020, 18:43 UTC
- Ora modificata: 05 giugno 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSWAFFullAccess

Descrizione: fornisce l'accesso completo alle azioni AWS WAF.

AWSWAFFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSWAFFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 ottobre 2015, 20:44 UTC
- Ora modificata: 05 giugno 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSWAFReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle azioni AWS WAF.

AWSWAFReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSWAFReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 ottobre 2015, 20:43 UTC
- Ora modificata: 05 giugno 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

Descrizione: consente di accedere WellArchitected a AWS servizi e risorse correlati alle WellArchitected risorse per conto dei clienti.

AWSWellArchitectedDiscoveryServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 26 aprile 2023, 18:36 UTC
- Ora modificata: 26 aprile 2023, 18:36 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:aws:servicecatalog:*:*:/applications/*",
        "arn:aws:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog>DeleteAttributeGroup"
    ],
    "Resource" : [
        "arn:aws:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

Descrizione: consente a Well-Architected di accedere a Organizations per tuo conto.

AWSWellArchitectedOrganizationsServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 giugno 2022, 17:15 UTC
- Ora modificata: 25 luglio 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSWickrFullAccess

Descrizione: Questa politica concede autorizzazioni amministrative complete al servizio Wickr, comprese le funzioni amministrative di Wickr ai sensi del. AWS Management Console

AWSWickrFullAccess [AWS è una politica](#) gestita.

Utilizzo di questa politica

Puoi collegarti AWSWickrFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 20:36 UTC
- Ora modificata: 27 novembre 2022, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
"Statement" : [  
  {  
    "Effect" : "Allow",  
    "Action" : "wickr:*",  
    "Resource" : "*"   
  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSXrayCrossAccountSharingConfiguration

Descrizione: Fornisce funzionalità per gestire i collegamenti di Observability Access Manager e stabilire la condivisione di tracce a raggi X

AWSXrayCrossAccountSharingConfiguration è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSXrayCrossAccountSharingConfiguration ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 13:46 UTC
- Ora modificata: 27 novembre 2022, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSXRayDaemonWriteAccess

Descrizione: consente al demone AWS X-Ray di inoltrare i dati grezzi dei segmenti di traccia all'API del servizio e di recuperare i dati di campionamento (regole, obiettivi, ecc.) da utilizzare con X-Ray SDK.

AWSXRayDaemonWriteAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti AWSXRayDaemonWriteAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 agosto 2018, 23:00 UTC
- Ora modificata: 13 febbraio 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AWSXRayDaemonWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingRules",
      "xray:GetSamplingTargets",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSXrayFullAccess

Descrizione: policy di accesso completo AWS gestito a X-Ray

AWSXrayFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSXrayFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 1 dicembre 2016, 18:30 UTC
- Ora modificata: 11 aprile 2024, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSXrayReadOnlyAccess

Descrizione: policy gestita in modalità di sola lettura AWS X-Ray

AWSXrayReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSXrayReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 18:27 UTC
- Ora modificata: 14 febbraio 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSXrayWriteOnlyAccess

Descrizione: policy AWS gestita solo in scrittura X-Ray

AWSXrayWriteOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti AWSXrayWriteOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 1 dicembre 2016, 18:19 UTC
- Ora modificata: 28 agosto 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

Descrizione: fornisce l'accesso amministrativo per le sessioni di esercitazione dei turni zonali ARC e l'accesso agli stati degli CloudWatch allarmi per monitorare le sessioni di pratica.

AWSZonalAutoshiftPracticeRunSLRPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 29 novembre 2023, 17:34 UTC
- Ora modificata: 29 novembre 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

BatchServiceRolePolicy

Descrizione: fornisce l'accesso al servizio AWS Batch per gestire le risorse richieste, incluse le risorse Amazon EC2 e Amazon ECS.

BatchServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 marzo 2021, 06:55 UTC
- Ora modificata: 05 dicembre 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
}
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

Billing

Descrizione: concede le autorizzazioni per la fatturazione e la gestione dei costi. Ciò include la visualizzazione dell'utilizzo dell'account e la visualizzazione e la modifica di budget e metodi di pagamento.

Billing è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti Billing ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:33 UTC
- Ora modificata: 23 maggio 2024, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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",
"ce:StartCostAllocationTagBackfill",
"ce:ListCostAllocationTagBackfillHistory",
"ce:GetTags",
"ce:GetDimensionValues",
"consolidatedbilling:GetAccountBillingRole",
"consolidatedbilling:ListLinkedAccounts",
"cur:DeleteReportDefinition",
"cur:DescribeReportDefinitions",
"cur:GetClassicReport",
"cur:GetClassicReportPreferences",
"cur:GetUsageReport",
"cur:ModifyReportDefinition",
"cur:PutClassicReportPreferences",
"cur:PutReportDefinition",
"cur:ValidateReportDestination",
"freetier:GetFreeTierAlertPreference",
"freetier:GetFreeTierUsage",
"freetier:PutFreeTierAlertPreference",
"invoicing:GetInvoiceEmailDeliveryPreferences",
"invoicing:GetInvoicePDF",
"invoicing:ListInvoiceSummaries",
"invoicing:PutInvoiceEmailDeliveryPreferences",
"payments:CreatePaymentInstrument",
"payments:DeletePaymentInstrument",
"payments:GetPaymentInstrument",
"payments:GetPaymentStatus",
"payments:ListPaymentPreferences",
"payments:ListTagsForResource",
"payments:ListPaymentInstruments",
```

```

    "payments:MakePayment",
    "payments:TagResource",
    "payments:UpdatePaymentPreferences",
    "payments:UpdatePaymentInstrument",
    "payments:UntagResource",
    "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" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CertificateManagerServiceRolePolicy

Descrizione: Politica sul ruolo del servizio Amazon Certificate Manager

CertificateManagerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 25 giugno 2020, 17:56 UTC
- Ora modificata: 25 giugno 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    "Action" : [
      "acm-pca:IssueCertificate",
      "acm-pca:GetCertificate"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ClientVPNServiceConnectionsRolePolicy

Descrizione: Politica per consentire a AWS Client VPN di gestire le connessioni degli endpoint Client VPN.

ClientVPNServiceConnectionsRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 agosto 2020, 19:48 UTC
- Ora modificata: 12 agosto 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ClientVPNServiceRolePolicy

Descrizione: Politica per consentire a AWS Client VPN di gestire gli endpoint Client VPN.

ClientVPNServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 dicembre 2018, 21:20 UTC

- Ora modificata: 12 agosto 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

Descrizione: Ruolo di servizio per CloudFormation StackSets (Organization Master Account)

CloudFormationStackSetsOrgAdminServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 dicembre 2019, 00:20 UTC
- Ora modificata: 10 dicembre 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

Descrizione: Ruolo di servizio per CloudFormation StackSets (account membro dell'organizzazione)

CloudFormationStackSetsOrgMemberServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 09 dicembre 2019, 23:52 UTC
- Ora modificata: 09 dicembre 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"  
    }  
  }  
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudFrontFullAccess

Descrizione: fornisce l'accesso completo alla CloudFront console oltre alla possibilità di elencare i bucket Amazon S3 tramite. AWS Management Console

CloudFrontFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudFrontFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 04 gennaio 2024, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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::*:*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudFrontReadOnlyAccess

Descrizione: fornisce l'accesso alle informazioni sulla configurazione CloudFront della distribuzione e alle distribuzioni degli elenchi tramite. AWS Management Console

CloudFrontReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudFrontReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 04 gennaio 2024, 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudHSMServiceRolePolicy

Descrizione: consente l'accesso alle AWS risorse utilizzate o gestite da CloudHSM

CloudHSMServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 6 novembre 2017, 19:12 UTC
- Ora modificata: 6 novembre 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
    ],  
    "Resource" : [  
        "arn:aws:logs:*:*:*"  
    ]  
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudSearchFullAccess

Descrizione: fornisce l'accesso completo al servizio CloudSearch di configurazione Amazon.

CloudSearchFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudSearchFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudSearchReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio di CloudSearch configurazione Amazon.

CloudSearchReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudSearchReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudTrailServiceRolePolicy

Descrizione: politica di autorizzazione per CloudTrail ServiceLinkedRole

CloudTrailServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 ottobre 2018, 21:21 UTC
- Ora modificata: 27 novembre 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
    }
  }
}

```

```
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatch-CrossAccountAccess

Descrizione: consente di CloudWatch assumere CloudWatch CrossAccountSharing ruoli in account remoti per conto dell'account corrente al fine di visualizzare i dati tra account diversi e tra regioni

CloudWatch-CrossAccountAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 luglio 2019, 09:59 UTC
- Ora modificata: 23 luglio 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchActionsEC2Access

Descrizione: fornisce accesso in sola lettura ad CloudWatch allarmi e metriche, nonché ai metadati EC2. Fornisce l'accesso alle istanze di Stop, Terminate e Reboot EC2.

CloudWatchActionsEC2Access [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti CloudWatchActionsEC2Access ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 luglio 2015, 00:00 UTC
- Ora modificata: 07 luglio 2015, 00:00 UTC

- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchAgentAdminPolicy

Descrizione: per l'utilizzo AmazonCloudWatchAgent sono necessarie autorizzazioni complete.

CloudWatchAgentAdminPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchAgentAdminPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 marzo 2018, 00:52 UTC
- Ora modificata: 05 febbraio 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchAgentServerPolicy

Descrizione: autorizzazioni necessarie per l'utilizzo AmazonCloudWatchAgent sui server

CloudWatchAgentServerPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchAgentServerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 7 marzo 2018, 01:06 UTC
- Ora modificata: 6 febbraio 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchApplicationInsightsFullAccess

Descrizione: fornisce l'accesso completo ad CloudWatch Application Insights e alle dipendenze richieste.

CloudWatchApplicationInsightsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchApplicationInsightsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 novembre 2020, 18:44 UTC
- Ora modificata: 25 gennaio 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchApplicationInsightsReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad CloudWatch Application Insights.

CloudWatchApplicationInsightsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchApplicationInsightsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 novembre 2020, 18:48 UTC

- Ora modificata: 24 novembre 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Descrizione: policy sui ruoli collegati del servizio Cloudwatch Application Insights

CloudwatchApplicationInsightsServiceLinkedRolePolicy è una policy [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 1 dicembre 2018, 16:22 UTC
- Ora modificata: 11 maggio 2023, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v24 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
    "*"
  ]
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchApplicationSignalsFullAccess

Descrizione: Fornisci l'accesso completo al servizio CloudWatch Application Signals e l'accesso mirato alle dipendenze necessarie per utilizzare e gestire questo servizio.

CloudWatchApplicationSignalsFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchApplicationSignalsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 giugno 2024, 22:50 UTC
- Ora modificata: 06 giugno 2024, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery",
```

```

        "logs:GetQueryResults"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
    "Effect" : "Allow",
    "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsRumPermissions",
    "Effect" : "Allow",
    "Action" : [
        "rum:BatchCreateRunMetricDefinitions",
        "rum:BatchDeleteRunMetricDefinitions",
        "rum:BatchGetRunMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRunMetricsDestination",
        "rum:UpdateRunMetricDefinition"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
    "Effect" : "Allow",
    "Action" : "xray:GetTraceSummaries",
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricAlarm",
    "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
    ]
}

```

```

    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns::*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
    }
  ]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchApplicationSignalsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al servizio CloudWatch Application Signals e l'accesso mirato alle dipendenze necessarie per utilizzare questo servizio

CloudWatchApplicationSignalsReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchApplicationSignalsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 giugno 2024, 22:48 UTC
- Ora modificata: 06 giugno 2024, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
```

```

        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
},
{
    "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
    "Effect" : "Allow",
    "Action" : [
        "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs::*:log-group:/aws/application-signals/data:*"
},
{
    "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
    "Effect" : "Allow",
    "Action" : [
        "logs:StopQuery",
        "logs:GetQueryResults"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "*"
},
{

```

```

    "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
    "Effect" : "Allow",
    "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
    "Effect" : "Allow",
    "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
    "Effect" : "Allow",
    "Action" : [
        "xray:GetTraceSummaries"
    ],
    "Resource" : "*"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchApplicationSignalsServiceRolePolicy

Descrizione: la politica concede l'autorizzazione ad CloudWatch Application Signals di raccogliere dati di monitoraggio e etichettatura da altri servizi pertinenti AWS .

CloudWatchApplicationSignalsServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 09 novembre 2023, 18:09 UTC
- Ora modificata: 26 aprile 2024, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Sid" : "XRayPermission",
"Effect" : "Allow",
"Action" : [
    "xray:GetServiceGraph"
],
"Resource" : [
    "*"
],
"Condition" : {
    "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
}
},
{
    "Sid" : "CWLogsPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "CWListMetricsPermission",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:ListMetrics"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
}
```

```
    }
  },
  {
    "Sid" : "CWGetMetricDataPermission",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "TagsPermission",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "EC2AutoScalingPermission",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:DescribeAutoScalingGroups"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
```

```
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchAutomaticDashboardsAccess

Descrizione: fornisce l'accesso alle non CloudWatch API utilizzate per visualizzare i dashboard CloudWatch automatici, incluso il contenuto di oggetti come le funzioni Lambda

CloudWatchAutomaticDashboardsAccess è [una policy gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchAutomaticDashboardsAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 luglio 2019, 10:01 UTC
- Ora modificata: 20 aprile 2021, 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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*"
    ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchCrossAccountSharingConfiguration

Descrizione: fornisce funzionalità per gestire i collegamenti di Observability Access Manager e stabilire la condivisione delle CloudWatch risorse

CloudWatchCrossAccountSharingConfiguration è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchCrossAccountSharingConfiguration ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 14:01 UTC
- Ora modificata: 27 novembre 2022, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchEventsBuiltInTargetExecutionAccess

Descrizione: consente ai target integrati in Amazon CloudWatch Events di eseguire azioni EC2 per tuo conto.

CloudWatchEventsBuiltInTargetExecutionAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchEventsBuiltInTargetExecutionAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 gennaio 2016, 18:35 UTC
- Ora modificata: 14 gennaio 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchEventsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon CloudWatch Events.

CloudWatchEventsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchEventsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 14 gennaio 2016, 18:37 UTC
- Ora modificata: 01 dicembre 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchEventsInvocationAccess

Descrizione: consente ad Amazon CloudWatch Events di inoltrare gli eventi agli stream in AWS Kinesis Streams del tuo account.

CloudWatchEventsInvocationAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti CloudWatchEventsInvocationAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 gennaio 2016, 18:36 UTC
- Ora modificata: 14 gennaio 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchEventsReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon CloudWatch Events.

CloudWatchEventsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchEventsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 14 gennaio 2016, 18:27 UTC
- Ora modificata: 01 dicembre 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchEventsServiceRolePolicy

Descrizione: consente di AWS CloudWatch eseguire azioni per conto dell'utente configurate tramite allarmi ed eventi.

CloudWatchEventsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 novembre 2017, 00:42 UTC
- Ora modificata: 17 novembre 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchFullAccess

Descrizione: Fornisce accesso completo a CloudWatch.

CloudWatchFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 27 novembre 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchFullAccessV2

Descrizione: Fornisce accesso completo a CloudWatch.

CloudWatchFullAccessV2 è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchFullAccessV2 ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 agosto 2023, 11:32 UTC
- Ora modificata: 17 maggio 2024, 22:20 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CloudWatchFullAccessPermissions",
    "Effect" : "Allow",
    "Action" : [
      "application-autoscaling:DescribeScalingPolicies",
      "application-signals:*",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribePolicies",
      "cloudwatch:*",
      "logs:*",
      "sns:CreateTopic",
      "sns:ListSubscriptions",
      "sns:ListSubscriptionsByTopic",
      "sns:ListTopics",
      "sns:Subscribe",
      "iam:GetPolicy",
      "iam:GetPolicyVersion",
      "iam:GetRole",
      "oam:ListSinks",
      "rum:*",
      "synthetics:*",
      "xray:*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "EventsServicePermissions",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "events.amazonaws.com"
        }
    }
},
{
    "Sid" : "OAMReadPermissions",
    "Effect" : "Allow",
    "Action" : [
        "oam:ListAttachedLinks"
    ],
    "Resource" : "arn:aws:oam::*:sink/*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchInternetMonitorServiceRolePolicy

Descrizione: consente a Internet Monitor di accedere a EC2, agli spazi di lavoro, CloudFront alle risorse e ad altri servizi richiesti per tuo conto.

CloudWatchInternetMonitorServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 27 novembre 2022, 17:46 UTC
- Ora modificata: 20 luglio 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchLambdaInsightsExecutionRolePolicy

Descrizione: policy richiesta per l'estensione Lambda Insights

CloudWatchLambdaInsightsExecutionRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchLambdaInsightsExecutionRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 ottobre 2020, 19:27 UTC
- Ora modificata: 07 ottobre 2020, 19:27 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchLogsCrossAccountSharingConfiguration

Descrizione: fornisce funzionalità per gestire i collegamenti di Observability Access Manager e stabilire la condivisione delle risorse dei CloudWatch log

CloudWatchLogsCrossAccountSharingConfiguration è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchLogsCrossAccountSharingConfiguration ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 13:55 UTC
- Ora modificata: 27 novembre 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  ]
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchLogsFullAccess

Descrizione: fornisce l'accesso completo ai CloudWatch registri

CloudWatchLogsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchLogsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 26 novembre 2023, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchLogsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ai CloudWatch registri

CloudWatchLogsReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchLogsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 26 novembre 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchNetworkMonitorServiceRolePolicy

Descrizione: consente a CloudWatch Network Monitor di accedere e gestire le risorse EC2 e VPC, pubblicare dati e accedere CloudWatch ad altri servizi richiesti per tuo conto.

CloudWatchNetworkMonitorServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 21 dicembre 2023, 18:53 UTC
- Ora modificata: 21 dicembre 2023, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a CloudWatch.

CloudWatchReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 17 maggio 2024, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",

```



```

        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*"
    ],
    "Resource" : "*"
},
{
    "Sid" : "OAMReadPermissions",
    "Effect" : "Allow",
    "Action" : [
        "oam:ListAttachedLinks"
    ],
    "Resource" : "arn:aws:oam:*:*:sink/*"
},
{
    "Sid" : "CloudWatchReadOnlyGetRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchSyntheticsFullAccess

Descrizione: Fornisce accesso completo a CloudWatch Synthetics.

CloudWatchSyntheticsFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchSyntheticsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 novembre 2019, 17:39 UTC
- Ora modificata: 06 maggio 2022, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CloudWatchSyntheticsReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura a CloudWatch Synthetics.

CloudWatchSyntheticsReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CloudWatchSyntheticsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 novembre 2019, 17:45 UTC
- Ora modificata: 6 marzo 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "synthetics:Describe*",
      "synthetics:Get*",
      "synthetics:List*"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ComprehendDataAccessRolePolicy

Descrizione: Policy for AWS Comprehend service role che consente l'accesso alle risorse S3 per l'accesso ai dati

ComprehendDataAccessRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ComprehendDataAccessRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 marzo 2019, 22:28 UTC
- Ora modificata: 6 marzo 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ComprehendFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Comprehend.

ComprehendFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `ComprehendFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 18:08 UTC
- Ora modificata: 5 dicembre 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ComprehendMedicalFullAccess

Descrizione: Fornisce accesso completo ad Amazon Comprehend Medical

ComprehendMedicalFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ComprehendMedicalFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 17:55 UTC
- Ora modificata: 27 novembre 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Action" : [
    "comprehendmedical:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ComprehendReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Comprehend.

ComprehendReadOnly [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti ComprehendReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 18:10 UTC
- Ora modificata: 26 aprile 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ComputeOptimizerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a ComputeOptimizer.

ComputeOptimizerReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ComputeOptimizerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 7 marzo 2020, 00:11 UTC
- Ora modificata: 28 agosto 2023, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ComputeOptimizerServiceRolePolicy

Descrizione: consente di ComputeOptimizer chiamare AWS i servizi e raccogliere i dettagli del carico di lavoro per tuo conto.

ComputeOptimizerServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 03 dicembre 2019, 08:45 UTC
- Ora modificata: 13 giugno 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ConfigConformsServiceRolePolicy

Descrizione: policy necessaria per AWSConfig creare pacchetti di conformità

ConfigConformsServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 25 luglio 2019, 21:38 UTC
- Ora modificata: 12 gennaio 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CostOptimizationHubAdminAccess

Descrizione: questa policy gestita fornisce l'accesso amministrativo al Cost Optimization Hub.

CostOptimizationHubAdminAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CostOptimizationHubAdminAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 dicembre 2023, 00:03 UTC
- Ora modificata: 19 dicembre 2023, 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CostOptimizationHubReadOnlyAccess

Descrizione: questa policy gestita fornisce l'accesso in sola lettura al Cost Optimization Hub.

CostOptimizationHubReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti CostOptimizationHubReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 dicembre 2023, 18:04 UTC
- Ora modificata: 13 dicembre 2023, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CostOptimizationHubServiceRolePolicy

Descrizione: consente a Cost Optimization Hub di recuperare le informazioni sull'organizzazione e raccogliere dati e metadati relativi all'ottimizzazione.

CostOptimizationHubServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi

- Ora di creazione: 26 novembre 2023, 08:03 UTC
- Ora modificata: 26 novembre 2023, 08:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

CustomerProfilesServiceLinkedRolePolicy

Descrizione: consente ai profili cliente di Amazon Connect di accedere a AWS servizi e risorse per tuo conto.

CustomerProfilesServiceLinkedRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 7 marzo 2023 22:56 UTC
- Ora modificata: 07 marzo 2023, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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_*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

DatabaseAdministrator

Descrizione: concede le autorizzazioni di accesso completo ai AWS servizi e alle azioni necessarie per impostare e configurare i servizi di AWS database.

DatabaseAdministrator è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti DatabaseAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:25 UTC
- Ora modificata: 08 gennaio 2019, 00:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

DataScientist

Descrizione: concede le autorizzazioni ai servizi di analisi AWS dei dati.

DataScientist è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti DataScientist ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:28 UTC
- Ora modificata: 03 dicembre 2019, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      ]
    }
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

DAXServiceRolePolicy

Descrizione: questa politica consente a DAX di creare e gestire l'interfaccia di rete, il gruppo di sicurezza, la sottorete e il Vpc per conto del cliente

DAXServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 marzo 2018, 17:51 UTC

- Ora modificata: 5 marzo 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Descrizione: autorizzazioni necessarie per supportare Amazon CloudWatch Contributor Insights per Amazon DynamoDB.

DynamoDBCloudWatchContributorInsightsServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 15 novembre 2019, 21:13 UTC
- Ora modificata: 15 novembre 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

DynamoDBKinesisReplicationServiceRolePolicy

Descrizione: Fornire l'accesso a AWS DynamoDB a KinesisDataStreams

DynamoDBKinesisReplicationServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 novembre 2020, 00:43 UTC
- Ora modificata: 12 novembre 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

DynamoDBReplicationServiceRolePolicy

Descrizione: Autorizzazioni richieste da DynamoDB per la replica dei dati tra regioni

DynamoDBReplicationServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 9 novembre 2017, 23:55 UTC
- Ora modificata: 08 gennaio 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
            ]
        }
    }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

EC2FastLaunchFullAccess

Descrizione: questa politica garantisce l'accesso completo alle azioni di EC2 Fast Launch

EC2FastLaunchFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti EC2FastLaunchFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 maggio 2024, 22:45 UTC
- Ora modificata: 13 maggio 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
      ],
      "Resource" : "*"
    }
  ],
}
```

```

{
  "Sid" : "EC2ReadOnly",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeImages",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSnapshots",
    "ec2:DescribeVolumes",
    "ec2:DescribeRegions",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeInstances",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeTags"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2LaunchInstance",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ]
},
{
  "Sid" : "EC2LaunchInstanceWithVolAndInstance",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {

```

```

        "StringEquals" : {
            "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
    },
    {
        "Sid" : "EC2Tags",
        "Effect" : "Allow",
        "Action" : "ec2:CreateTags",
        "Resource" : [
            "arn:aws:ec2:*:*:volume/*",
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:snapshot/*",
            "arn:aws:ec2:*:*:launch-template/*",
            "arn:aws:ec2:*:*:vpc/*",
            "arn:aws:ec2:*:*:subnet/*"
        ],
        "Condition" : {
            "StringEquals" : {
                "ec2:CreateAction" : "RunInstances"
            }
        }
    },
    {
        "Sid" : "IAMSLR",
        "Effect" : "Allow",
        "Action" : "iam:CreateServiceLinkedRole",
        "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/AWSServiceRoleForEC2FastLaunch",
        "Condition" : {
            "StringLike" : {
                "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
            }
        }
    },
    {
        "Sid" : "IAMSLRPassRole",
        "Effect" : "Allow",
        "Action" : "iam:PassRole",
        "Resource" : [
            "arn:aws:iam::*:instance-profile/*",
            "arn:aws:iam::*:role/*"
        ],
        "Condition" : {

```

```
"StringEquals" : {
  "iam:PassedToService" : [
    "ec2.amazonaws.com",
    "ec2.amazonaws.com.cn"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

EC2FastLaunchServiceRolePolicy

Descrizione: la politica consente a ec2fastlaunch di preparare e gestire istantanee preimpostate nell'account del cliente e pubblicare le relative metriche.

EC2FastLaunchServiceRolePolicy è una [AWS politica](#) gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 gennaio 2022, 13:08 UTC
- Ora modificata: 10 gennaio 2022, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:DescribeInstanceStatus",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypeOfferings",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribeLaunchTemplates"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/EC2"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

EC2FleetTimeShiftableServiceRolePolicy

Descrizione: politica che concede le autorizzazioni a EC2 Fleet per lanciare istanze in futuro.

EC2FleetTimeShiftableServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 23 dicembre 2019, 19:47 UTC
- Ora modificata: 23 dicembre 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

Ec2ImageBuilderCrossAccountDistributionAccess

Descrizione: le autorizzazioni necessarie a EC2 Image Builder per eseguire una distribuzione tra account.

Ec2ImageBuilderCrossAccountDistributionAccess [è una politica gestita AWS](#) .

Utilizzo di questa politica

Puoi collegarti Ec2ImageBuilderCrossAccountDistributionAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2020, 19:22 UTC
- Ora modificata: 30 settembre 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

EC2ImageBuilderLifecycleExecutionPolicy

Descrizione: la ImageBuilderLifecycleExecutionPolicy policy EC2 concede le autorizzazioni a Image Builder per eseguire azioni come deprecare o eliminare le risorse di immagine di Image Builder e le relative risorse sottostanti (AMI, istantanee) per supportare regole automatizzate per le attività di gestione del ciclo di vita delle immagini.

EC2ImageBuilderLifecycleExecutionPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti EC2ImageBuilderLifecycleExecutionPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 16 novembre 2023, 23:23 UTC
- Ora modificata: 16 novembre 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

EC2InstanceConnect

Descrizione: consente ai clienti di chiamare EC2 Instance Connect per pubblicare chiavi temporanee sulle proprie istanze EC2 e connettersi tramite ssh o l'EC2 Instance Connect CLI.

EC2InstanceConnect [è una policy gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti EC2InstanceConnect ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2019, 18:53 UTC
- Ora modificata: 27 giugno 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

Ec2InstanceConnectEndpoint

Descrizione: policy degli endpoint EC2 Instance Connect per gestire gli endpoint EC2 Instance Connect creati dal cliente

Ec2InstanceConnectEndpoint [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 gennaio 2023, 20:19 UTC
- Ora modificata: 24 gennaio 2023, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
            ]
        }
    }
}
]
}
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

EC2InstanceProfileForImageBuilder

Descrizione: profilo di istanza EC2 per il servizio Image Builder.

EC2InstanceProfileForImageBuilder è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `EC2InstanceProfileForImageBuilder` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2019, 19:08 UTC
- Ora modificata: 27 agosto 2020, 16:40 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

Descrizione: profilo di istanza EC2 per la creazione di immagini di container con EC2 Image Builder. Questa politica concede all'utente ampie autorizzazioni per caricare immagini ECR.

EC2InstanceProfileForImageBuilderECRContainerBuilds è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti `EC2InstanceProfileForImageBuilderECRContainerBuilds` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2020, 19:48 UTC
- Ora modificata: 11 dicembre 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ECRReplicationServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da ECR Replication

ECRReplicationServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 4 dicembre 2020, 22:11 UTC
- Ora modificata: 04 dicembre 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ]
    }
  ],
}
```

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElastiCacheServiceRolePolicy

Descrizione: questa politica consente di ElastiCache gestire AWS le risorse per conto dell'utente nella misura necessaria alla gestione della cache

ElastiCacheServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 7 dicembre 2017, 17:50 UTC
- Ora modificata: 28 novembre 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    }
  ]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElasticLoadBalancingFullAccess

Descrizione: fornisce accesso completo ad Amazon ElasticLoadBalancing e accesso limitato ad altri servizi necessari per fornire ElasticLoadBalancing funzionalità.

ElasticLoadBalancingFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ElasticLoadBalancingFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 settembre 2018, 20:42 UTC
- Ora modificata: 29 novembre 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElasticLoadBalancingReadOnly

Descrizione: Fornisce accesso in sola lettura ad Amazon ElasticLoadBalancing e ai servizi dipendenti

ElasticLoadBalancingReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ElasticLoadBalancingReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 20 settembre 2018, 20:17 UTC
- Ora modificata: 26 novembre 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElementalActivationsDownloadSoftwareAccess

Descrizione: Accesso per visualizzare gli asset acquistati e scaricare il software correlato e i file kickstart

ElementalActivationsDownloadSoftwareAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ElementalActivationsDownloadSoftwareAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 8 settembre 2020, 17:26 UTC
- Ora modificata: 08 settembre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "*"br/>  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElementalActivationsFullAccess

Descrizione: accesso completo alla visualizzazione e all'adozione di misure relative alle apparecchiature elementari e ai software acquistati

ElementalActivationsFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ElementalActivationsFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 giugno 2020, 21:00 UTC
- Ora modificata: 4 giugno 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElementalActivationsGenerateLicenses

Descrizione: accesso per visualizzare gli asset acquistati e generare licenze software per le attivazioni in sospeso

ElementalActivationsGenerateLicenses [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti ElementalActivationsGenerateLicenses ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 agosto 2020, 18:28 UTC

- Ora modificata: 28 agosto 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElementalActivationsReadOnlyAccess

Descrizione: accesso in sola lettura all'elenco dettagliato degli asset acquistati associati all' Account AWS utente

ElementalActivationsReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ElementalActivationsReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 28 agosto 2020, 16:51 UTC
- Ora modificata: 28 agosto 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElementalAppliancesSoftwareFullAccess

Descrizione: accesso completo per visualizzare e intervenire sui preventivi e sugli ordini di elettrodomestici e software elementali

ElementalAppliancesSoftwareFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ElementalAppliancesSoftwareFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 31 luglio 2019, 16:28 UTC
- Ora modificata: 5 febbraio 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElementalAppliancesSoftwareReadOnlyAccess

Descrizione: accesso in sola lettura per visualizzare i preventivi e gli ordini di elettrodomestici e software elementali

ElementalAppliancesSoftwareReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti ElementalAppliancesSoftwareReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2020, 22:31 UTC
- Ora modificata: 01 aprile 2020, 22:31 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ElementalSupportCenterFullAccess

Descrizione: accesso completo per visualizzare e intervenire sui casi di supporto relativi a dispositivi e software Elemental Appliance e ai contenuti di supporto ai prodotti

ElementalSupportCenterFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `ElementalSupportCenterFullAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 novembre 2020, 18:08 UTC
- Ora modificata: 5 febbraio 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

EMRDescribeClusterPolicyForEMRWAL

Descrizione: questa politica concede autorizzazioni di sola lettura che consentono al servizio WAL per Amazon EMR di trovare e restituire lo stato di un cluster

EMRDescribeClusterPolicyForEMRWAL [AWS è una politica](#) gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 15 giugno 2023, 23:30 UTC
- Ora modificata: 15 giugno 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:DescribeCluster"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

FMSServiceRolePolicy

Descrizione: politica di accesso per consentire al ruolo collegato al servizio FM di eseguire azioni relative a FM sulle risorse gestite da FM all'interno dell'account dell'organizzazione del cliente. AWS

FMSServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 28 marzo 2018, 23:01 UTC
- Ora modificata: 22 aprile 2024, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Versione della politica

Versione della politica: v29 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*:*/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
```

```

    "Effect" : "Allow",
    "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2>DeleteLoggingConfiguration"
    ],
    "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
    ]
},
{
    "Sid" : "WafWebaclCreation",
    "Effect" : "Allow",
    "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
    ],
    "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
    ]
},
{
    "Sid" : "ElbGeneral",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
    ],
    "Resource" : "*"
},
{
    "Sid" : "WafPermissionPolicy",
    "Effect" : "Allow",
    "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf>DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",

```

```

        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
    ],
    "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
    ]
},
{
    "Sid" : "CloudfrontGeneral",
    "Effect" : "Allow",
    "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ConfigScoped",
    "Effect" : "Allow",
    "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation",
        "config:DeleteEvaluationResults"
    ],
    "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/"
}
*
},
{
    "Sid" : "ConfigUnscoped",
    "Effect" : "Allow",
    "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",

```

```

        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig"
    ],
    "Resource" : "*"
},
{
    "Sid" : "SlrDeletion",
    "Effect" : "Allow",
    "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
    ]
},
{
    "Sid" : "OrganizationsGeneral",
    "Effect" : "Allow",
    "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "ShieldGeneral",
    "Effect" : "Allow",

```



```

    "Action" : [
      "shield:CreateProtection",
      "shield>DeleteProtection",
      "shield:DescribeProtection",
      "shield>ListProtections",
      "shield>ListAttacks",
      "shield>CreateSubscription",
      "shield:DescribeSubscription",
      "shield:GetSubscriptionState",
      "shield:DescribeDRTAccess",
      "shield:DescribeEmergencyContactSettings",
      "shield:UpdateEmergencyContactSettings",
      "elasticloadbalancing:DescribeLoadBalancers",
      "ec2:DescribeAddresses",
      "shield:EnableApplicationLayerAutomaticResponse",
      "shield:DisableApplicationLayerAutomaticResponse",
      "shield:UpdateApplicationLayerAutomaticResponse"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2SecurityGroupScoped",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2>DeleteSecurityGroup",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
      "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Sid" : "SecurityGroupTagCreation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ]
  },

```

```

    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSecurityGroup"
      }
    }
  },
  {
    "Sid" : "SecurityGroupTagManagement",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteTags",
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/FMManaged" : "*"
      }
    }
  },
  {
    "Sid" : "Ec2Unscoped",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup",
      "ec2:DescribeSecurityGroupReferences",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeStaleSecurityGroups",
      "ec2:DescribeNetworkInterfaces",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcPeeringConnections",
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeInstances",
      "ec2:AssociateRouteTable",
      "ec2:CreateSubnet",
      "ec2:CreateRouteTable",
      "ec2>DeleteSubnet",
      "ec2:DisassociateRouteTable",

```

```

    "ec2:ReplaceRouteTableAssociation"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "Wafv2General",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:TagResource",
    "wafv2:ListResourcesForWebACL",
    "wafv2:AssociateWebACL",
    "wafv2:ListTagsForResource",
    "wafv2:UntagResource",
    "wafv2:GetWebACL",
    "wafv2:DisassociateFirewallManager",
    "wafv2>DeleteWebACL",
    "wafv2:DisassociateWebACL"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:global/webacl/*",
    "arn:aws:wafv2:*:*:regional/webacl/*"
  ]
},
{
  "Sid" : "Wafv2WebAclAndRuleGroupMutation",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:UpdateWebACL",
    "wafv2>CreateWebACL",
    "wafv2>DeleteFirewallManagerRuleGroups",
    "wafv2:PutFirewallManagerRuleGroups"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:global/webacl/*",
    "arn:aws:wafv2:*:*:regional/webacl/*",
    "arn:aws:wafv2:*:*:global/rulegroup/*",
    "arn:aws:wafv2:*:*:regional/rulegroup/*",
    "arn:aws:wafv2:*:*:global/managedruleset/*",
    "arn:aws:wafv2:*:*:regional/managedruleset/*",
    "arn:aws:wafv2:*:*:global/ipset/*",
    "arn:aws:wafv2:*:*:regional/ipset/*",
    "arn:aws:wafv2:*:*:global/regexpatternset/*",

```

```

        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
    ],
},
{
    "Sid" : "Wafv2PermissionPolicy",
    "Effect" : "Allow",
    "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2>DeletePermissionPolicy"
    ],
    "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
    ]
},
{
    "Sid" : "Wafv2WebaclDescribe",
    "Effect" : "Allow",
    "Action" : [
        "wafv2:GetWebACLForResource"
    ],
    "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
    ]
},
{
    "Sid" : "RouteTableTagManagement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
        "StringEquals" : {
            "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "Name",
                "FMManaged"
            ]
        }
    }
},
{

```

```
    "Sid" : "SubnetTagManagement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
    ],
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "Name",
                "FMManaged"
            ]
        }
    }
},
{
    "Sid" : "VPCEndpointTagManagement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "Name",
                "FMManaged"
            ]
        }
    }
},
{
    "Sid" : "RouteTableCleanup",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteRouteTable",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
        "StringEquals" : {
            "ec2:ResourceTag/FMManaged" : "true"
        }
    }
}
```

```
    },
    {
      "Sid" : "Ec2DescribeUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateVpcEndpointScoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "CreateVpcEndpointUnscoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VpcEndpointsDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
```

```
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/FMManaged" : "true"
      }
    }
  },
  {
    "Sid" : "RamTagManagement",
    "Effect" : "Allow",
    "Action" : [
      "ram:TagResource"
    ],
    "Resource" : [
      "arn:aws:ram:*:*:resource-share/*"
    ],
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "Name",
          "FMManaged"
        ]
      }
    }
  },
  {
    "Sid" : "RamMutation",
    "Effect" : "Allow",
    "Action" : [
      "ram:AssociateResourceShare",
      "ram:UpdateResourceShare",
      "ram>DeleteResourceShare"
    ],
    "Resource" : "arn:aws:ram:*:*:resource-share/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/FMManaged" : "true"
      }
    }
  },
  {
    "Sid" : "RamCreation",
    "Effect" : "Allow",
    "Action" : "ram:CreateResourceShare",
```

```
"Resource" : "*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "Name",
      "FMManaged"
    ]
  },
  "StringEquals" : {
    "aws:RequestTag/FMManaged" : [
      "true"
    ]
  }
},
{
  "Sid" : "RamDescribe",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShareAssociations",
    "ram:GetResourceShares"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SlrCreation",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "network-firewall.amazonaws.com",
        "shield.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "IamDescribe",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "*"
},
```



```

{
  "Sid" : "NetworkFirewallTagManagement",
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Sid" : "NetworkFirewallGeneral",
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:AssociateSubnets",
    "network-firewall:CreateFirewall",
    "network-firewall:CreateFirewallPolicy",
    "network-firewall:DisassociateSubnets",
    "network-firewall:UpdateFirewallDeleteProtection",
    "network-firewall:UpdateFirewallPolicy",
    "network-firewall:UpdateFirewallPolicyChangeProtection",
    "network-firewall:UpdateSubnetChangeProtection",
    "network-firewall:AssociateFirewallPolicy",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "network-firewall:PutResourcePolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall>DeleteResourcePolicy",
    "network-firewall:DescribeLoggingConfiguration",
    "network-firewall:UpdateLoggingConfiguration"
  ],
  "Resource" : "*"
},
{

```

```

    "Sid" : "NetworkFirewallCleanup",
    "Effect" : "Allow",
    "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/FMManaged" : "true"
        }
    }
},
{
    "Sid" : "LogsGeneral",
    "Effect" : "Allow",
    "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Route53ResolverRuleGroupUnscoped",
    "Effect" : "Allow",
    "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Route53ResolverRuleGroupCleanup",
    "Effect" : "Allow",
    "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",

```

```

        "route53resolver:DisassociateFirewallRuleGroup"
    ],
    "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/FMManaged" : "true"
        }
    }
},
{
    "Sid" : "Route53ResolverRuleGroupScoped",
    "Effect" : "Allow",
    "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
    ],
    "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/FMManaged" : "true"
        }
    }
},
{
    "Sid" : "NaclTagCreation",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-acl/*",
    "Condition" : {
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "Name",
                "FMManaged",
                "FMPolicies"
            ]
        },
        "StringEquals" : {
            "ec2:CreateAction" : "CreateNetworkAcl"
        }
    }
},
{

```

```
"Sid" : "NaclTagManagement",
"Effect" : "Allow",
"Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
],
"Resource" : "arn:aws:ec2:*:*:network-acl/*",
"Condition" : {
    "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
        ]
    },
    "StringEquals" : {
        "aws:ResourceTag/FMManaged" : "true"
    }
}
},
{
    "Sid" : "NaclScoped",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteNetworkAclEntry",
        "ec2:CreateNetworkAclEntry",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/FMManaged" : "true"
        }
    }
}
},
{
    "Sid" : "NaclUnscoped",
    "Effect" : "Allow",
    "Action" : [
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateNetworkAcl"
    ]
},
```

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

FSxDeleteServiceLinkedRoleAccess

Descrizione: consente ad Amazon FSx di eliminare i ruoli collegati ai servizi per l'accesso ad Amazon S3

FSxDeleteServiceLinkedRoleAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 28 novembre 2018, 10:40 UTC
- Ora modificata: 28 novembre 2018, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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_*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

GameLiftGameServerGroupPolicy

Descrizione: Politica per consentire a Gamelift di GameServerGroups gestire le risorse dei clienti

GameLiftGameServerGroupPolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti GameLiftGameServerGroupPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 03 aprile 2020, 23:12 UTC
- Ora modificata: 13 maggio 2020, 17:27 UTC

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

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:aws:sns:***:ActivatingLifecycleHookTopic-***",
        "arn:aws:sns:***:TerminatingLifecycleHookTopic-***"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
    }
  ]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

GlobalAcceleratorFullAccess

Descrizione: consenti GlobalAccelerator agli utenti l'accesso completo a tutte le API

GlobalAcceleratorFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti GlobalAcceleratorFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 02:44 UTC
- Ora modificata: 04 dicembre 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

GlobalAcceleratorReadOnlyAccess

Descrizione: consenti GlobalAccelerator agli utenti l'accesso alle API di sola lettura

GlobalAcceleratorReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `GlobalAcceleratorReadOnlyAccess` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 02:41 UTC
- Ora modificata: 27 novembre 2018, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

GreengrassOTAUpdateArtifactAccess

Descrizione: Fornisce l'accesso in lettura agli artefatti Greengrass OTA Update in tutte le regioni Greengrass

GreengrassOTAUpdateArtifactAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti GreengrassOTAUpdateArtifactAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 novembre 2017, 18:11 UTC
- Ora modificata: 18 dicembre 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*-greengrass-updates/*"
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

GroundTruthSyntheticConsoleFullAccess

Descrizione: questa politica concede le autorizzazioni necessarie per utilizzare tutte le funzionalità della console sintetica SageMaker Ground Truth.

GroundTruthSyntheticConsoleFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti GroundTruthSyntheticConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 agosto 2022, 15:58 UTC
- Ora modificata: 25 agosto 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

GroundTruthSyntheticConsoleReadOnlyAccess

Descrizione: Questa politica garantisce l'accesso in sola lettura a SageMaker Ground Truth Synthetic tramite AWS Management Console.

GroundTruthSyntheticConsoleReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti GroundTruthSyntheticConsoleReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 25 agosto 2022, 15:58 UTC
- Ora modificata: 25 agosto 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

Health_OrganizationsServiceRolePolicy

Descrizione: policy AWS Health per abilitare la funzionalità Organizational View

Health_OrganizationsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 dicembre 2019, 13:28 UTC
- Ora modificata: 6 febbraio 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
```



```
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
    ],
    "Resource" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IAMAccessAdvisorReadOnly

Descrizione: questa policy consente l'accesso alla lettura di tutte le informazioni di accesso fornite da IAM Access Advisor, come le informazioni sull'ultimo accesso al servizio.

IAMAccessAdvisorReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti IAMAccessAdvisorReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 21 giugno 2019, 19:33 UTC
- Ora modificata: 21 giugno 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IAMAccessAnalyzerFullAccess

Descrizione: fornisce l'accesso completo a IAM Access Analyzer

IAMAccessAnalyzerFullAccess è una [policy AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti IAMAccessAnalyzerFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2019, 17:12 UTC
- Ora modificata: 02 dicembre 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IAMAccessAnalyzerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle risorse di IAM Access Analyzer

IAMAccessAnalyzerReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti IAMAccessAnalyzerReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2019, 17:12 UTC
- Ora modificata: 27 novembre 2023, 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IAMFullAccess

Descrizione: fornisce l'accesso completo a IAM tramite AWS Management Console.

IAMFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti IAMFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 21 giugno 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IAMReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a IAM tramite AWS Management Console.

IAMReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti IAMReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 25 gennaio 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IAMSelfManageServiceSpecificCredentials

Descrizione: consente a un utente IAM di gestire le proprie credenziali specifiche del servizio.

IAMSelfManageServiceSpecificCredentials è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti IAMSelfManageServiceSpecificCredentials ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 dicembre 2016, 17:25 UTC
- Ora modificata: 22 dicembre 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IAMUserChangePassword

Descrizione: offre la possibilità a un utente IAM di modificare la propria password.

IAMUserChangePassword è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti IAMUserChangePassword ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2016, 00:25 UTC
- Ora modificata: 15 novembre 2016, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IAMUserSSHKeys

Descrizione: offre la possibilità a un utente IAM di gestire le proprie chiavi SSH.

IAMUserSSHKeys è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti IAMUserSSHKeys ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:08 UTC
- Ora modificata: 9 luglio 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IVSFullAccess

Descrizione: fornisce l'accesso completo a Interactive Video Service (IVS), include anche le autorizzazioni per i servizi dipendenti, necessarie per l'accesso completo alla console ivs.

IVSFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti IVSFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 13 dicembre 2023, 21:20 UTC
- Ora modificata: 13 dicembre 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Action" : [
    "ivs:*",
    "ivschat:*"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IVSReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle API di streaming IVS a bassa latenza e in tempo reale

IVSReadOnlyAccess è [AWS una](#) politica gestita.

Utilizzo di questa politica

Puoi collegarti IVSReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 5 dicembre 2023, 18:00 UTC
- Ora modificata: 16 febbraio 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ],
  "Resource" : "*"
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

IVSRecordToS3

Descrizione: Service Linked Role per eseguire da S3 PutObject alla registrazione di live streaming IVS

IVSRecordToS3 [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 dicembre 2020, 00:10 UTC
- Ora modificata: 05 dicembre 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

KafkaConnectServiceRolePolicy

Descrizione: questa politica concede a Kafka Connect l'autorizzazione a AWS gestire le risorse per tuo conto.

KafkaConnectServiceRolePolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 07 settembre 2021, 13:12 UTC

- Ora modificata: 07 settembre 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

KafkaServiceRolePolicy

Descrizione: politica dei ruoli collegati al servizio IAM per Kafka.

KafkaServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 15 novembre 2018, 23:31 UTC
- Ora modificata: 28 aprile 2023, 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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_*"
    }
  }
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

KeyspacesReplicationServiceRolePolicy

Descrizione: autorizzazioni richieste da Keyspaces per la replica dei dati tra regioni

KeyspacesReplicationServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 2 maggio 2023, 16:15 UTC
- Ora modificata: 2 maggio 2023, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "cassandra:Select",
      "cassandra:SelectMultiRegionResource",
      "cassandra:Modify",
      "cassandra:ModifyMultiRegionResource"
    ],
    "Resource" : "*"
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

LakeFormationDataAccessServiceRolePolicy

Descrizione: Politica per concedere l'accesso temporaneo ai dati alle risorse di Lake Formation

LakeFormationDataAccessServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 20 giugno 2019, 20:46 UTC
- Ora modificata: 6 febbraio 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

LexBotPolicy

Descrizione: Policy per il caso d'uso di AWS Lex Bot

LexBotPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 febbraio 2017, 22:18 UTC
- Ora modificata: 13 novembre 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

LexChannelPolicy

Descrizione: Policy per il caso d'uso di AWS Lex Channel

LexChannelPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 febbraio 2017, 23:23 UTC
- Ora modificata: 17 febbraio 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

LightsailExportAccess

Descrizione: AWS politica dei ruoli collegati al servizio Lightsail che concede le autorizzazioni per esportare risorse

LightsailExportAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 28 settembre 2018, 16:35 UTC
- Ora modificata: 15 gennaio 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

MediaConnectGatewayInstanceRolePolicy

Descrizione: questa politica concede l'autorizzazione a registrare le istanze MediaConnect Gateway su un MediaConnect Gateway.

MediaConnectGatewayInstanceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti MediaConnectGatewayInstanceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 22 marzo 2023, 20:43 UTC
- Ora modificata: 22 marzo 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
{
  "Sid" : "MediaConnectGateway",
  "Effect" : "Allow",
  "Action" : [
    "mediaconnect:DiscoverGatewayPollEndpoint",
    "mediaconnect:PollGateway",
    "mediaconnect:SubmitGatewayStateChange"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

MediaPackageServiceRolePolicy

Descrizione: consente MediaPackage di pubblicare registri su CloudWatch

MediaPackageServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 settembre 2020, 17:45 UTC
- Ora modificata: 18 settembre 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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/*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

MemoryDBServiceRolePolicy

Descrizione: questa politica consente a MemoryDB di gestire AWS le risorse per conto dell'utente nella misura necessaria per la gestione delle risorse.

MemoryDBServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 17 agosto 2021, 22:34 UTC
- Ora modificata: 18 agosto 2021, 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

MigrationHubDMSAccessServiceRolePolicy

Descrizione: Politica per l'assunzione del ruolo del Database Migration Service nell'account del cliente per chiamare Migration Hub

MigrationHubDMSAccessServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 giugno 2019, 17:50 UTC

- Ora modificata: 07 ottobre 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

MigrationHubServiceRolePolicy

Descrizione: consente a Migration Hub di chiamare Application Discovery Service per conto dell'utente

MigrationHubServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 giugno 2019, 17:22 UTC
- Ora modificata: 06 agosto 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

MigrationHubSMSAccessServiceRolePolicy

Descrizione: Politica per l'assunzione del ruolo del servizio di migrazione dei server nell'account del cliente per chiamare Migration Hub

MigrationHubSMSAccessServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 giugno 2019, 18:30 UTC
- Ora modificata: 07 ottobre 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

MonitronServiceRolePolicy

Descrizione: Policy per il ruolo collegato al servizio AWS Monitron che garantisce l'accesso alle risorse richieste del cliente.

MonitronServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 2 maggio 2022, 19:22 UTC
- Ora modificata: 02 maggio 2022, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

NeptuneConsoleFullAccess

Descrizione: fornisce l'accesso completo per gestire Amazon Neptune utilizzando AWS Management Console. Tieni presente che questa policy garantisce anche l'accesso completo alla pubblicazione su tutti gli argomenti SNS all'interno dell'account, le autorizzazioni per creare e modificare istanze Amazon EC2 e configurazioni VPC, le autorizzazioni per visualizzare ed elencare le chiavi su Amazon KMS e l'accesso completo ad Amazon RDS. Per ulteriori informazioni, consulta <https://aws.amazon.com/neptune/faqs/>.

NeptuneConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti NeptuneConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 19 giugno 2018, 21:35 UTC
- Ora modificata: 30 novembre 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:RemoveTagsForResource",
        "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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

NeptuneFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Neptune. Tieni presente che questa politica garantisce anche l'accesso completo alla pubblicazione su tutti gli argomenti SNS all'interno dell'account e l'accesso completo ad Amazon RDS. Per ulteriori informazioni, consulta <https://aws.amazon.com/neptune/faqs/>.

NeptuneFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti NeptuneFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2018, 19:17 UTC
- Ora modificata: 22 gennaio 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

NeptuneGraphReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a tutte le risorse di Amazon Neptune Analytics insieme alle autorizzazioni di sola lettura per i servizi dipendenti.

NeptuneGraphReadOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti NeptuneGraphReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2023, 07:32 UTC
- Ora modificata: 30 novembre 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

NeptuneReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Neptune. Tieni presente che questa politica consente anche l'accesso alle risorse Amazon RDS. Per ulteriori informazioni, consulta <https://aws.amazon.com/neptune/faqs/>.

NeptuneReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti NeptuneReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2018, 19:16 UTC
- Ora modificata: 22 gennaio 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : [
        "*"
    ]
}
}

```

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

NetworkAdministrator

Descrizione: concede le autorizzazioni di accesso completo ai AWS servizi e alle azioni necessarie per impostare e configurare le risorse di AWS rete.

NetworkAdministrator è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti NetworkAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:31 UTC
- Ora modificata: 16 settembre 2021, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

OAMFullAccess

Descrizione: fornisce l'accesso completo a CloudWatch Observability Access Manager

OAMFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti OAMFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 13:38 UTC
- Ora modificata: 27 novembre 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

OAMReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a CloudWatch Observability Access Manager

OAMReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti OAMReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 13:29 UTC
- Ora modificata: 27 novembre 2022, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

OpensearchIngestionSelfManagedVpcePolicy

Descrizione: consente ad Amazon OpenSearch Ingestion di descrivere le risorse di rete e scrivere metriche di servizio su cloudwatch

OpensearchIngestionSelfManagedVpcePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 10 giugno 2024, 19:59 UTC
- Ora modificata: 10 giugno 2024, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CwPermissionsForOsiNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

PartnerCentralAccountManagementUserRoleAssociation

Descrizione: fornisce l'accesso per associare e dissociare gli utenti di Partner Central con ruoli IAM

PartnerCentralAccountManagementUserRoleAssociation è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `PartnerCentralAccountManagementUserRoleAssociation` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2023, 02:03 UTC
- Ora modificata: 10 novembre 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

PowerUserAccess

Descrizione: fornisce l'accesso completo ai AWS servizi e alle risorse, ma non consente la gestione di utenti e gruppi.

PowerUserAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti PowerUserAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 06 luglio 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

QBusinessServiceRolePolicy

Descrizione: concede autorizzazioni Servizi AWS e risorse utilizzate o gestite da Amazon Q

QBusinessServiceRolePolicy è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 29 aprile 2024, 16:05 UTC
- Ora modificata: 29 aprile 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "cloudwatch:namespace" : "AWS/QBusiness"
        }
    }
},
{
    "Sid" : "QBusinessCreateLogGroupPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogGroup"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "QBusinessDescribeLogGroupsPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:DescribeLogGroups"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "QBusinessLogStreamPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
}
```

```
{
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Descrizione: politica utilizzata dal QuickSight team per accedere ai dati dei clienti prodotti da S3 Storage Management Analytics.

QuickSightAccessForS3StorageManagementAnalyticsReadOnly è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti QuickSightAccessForS3StorageManagementAnalyticsReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 giugno 2017, 18:18 UTC
- Ora modificata: 08 ottobre 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

RDSCloudHsmAuthorizationRole

Descrizione: policy predefinita per il ruolo del servizio Amazon RDS.

RDSCloudHsmAuthorizationRole è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti RDSCloudHsmAuthorizationRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 26 settembre 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "*"br/>  }  
]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a AWS servizi e risorse.

ReadOnlyAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 16 maggio 2024, 21:10 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Versione della politica

Versione della politica: v113 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:BatchGetLifecyclePolicy",
"aoss:BatchGetVpcEndpoint",
"aoss:GetAccessPolicy",
"aoss:GetAccountSettings",
"aoss:GetPoliciesStats",
"aoss:GetSecurityConfig",
"aoss:GetSecurityPolicy",
"aoss:ListAccessPolicies",
"aoss:ListCollections",
"aoss:ListLifecyclePolicies",
"aoss:ListSecurityConfigs",
"aoss:ListSecurityPolicies",
"aoss:ListTagsForResource",
"aoss:ListVpcEndpoints",
"apigateway:GET",
"appconfig:GetApplication",
"appconfig:GetConfiguration",
"appconfig:GetConfigurationProfile",
"appconfig:GetDeployment",
"appconfig:GetDeploymentStrategy",
"appconfig:GetEnvironment",
"appconfig: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:DescribeWebAclForService",
"apprunner:ListAssociatedServicesForWebAcl",
"apprunner:ListAutoScalingConfigurations",
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListServicesForAutoScalingConfiguration",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appstream:Describe*",
"appstream:List*",
"appsync:Get*",
"appsync:List*",
"aps:DescribeAlertManagerDefinition",
"aps:DescribeLoggingConfiguration",
```

```
"aps:DescribeRuleGroupsNamespace",
"aps:DescribeScraper",
"aps:DescribeWorkspace",
"aps:GetAlertManagerSilence",
"aps:GetAlertManagerStatus",
"aps:GetDefaultScraperConfiguration",
"aps:GetLabels",
"aps:GetMetricMetadata",
"aps:GetSeries",
"aps:ListAlertManagerAlertGroups",
"aps:ListAlertManagerAlerts",
"aps:ListAlertManagerReceivers",
"aps:ListAlertManagerSilences",
"aps:ListAlerts",
"aps:ListRuleGroupsNamespaces",
"aps:ListRules",
"aps:ListScrapers",
"aps:ListTagsForResource",
"aps:ListWorkspaces",
"aps:QueryMetrics",
"arc-zonal-shift: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:ListCostAllocationTagBackfillHistory",
"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:GetConfiguredAudienceModelAssociation",
```

```
"cleanrooms:GetConfiguredTable",
"cleanrooms:GetConfiguredTableAnalysisRule",
"cleanrooms:GetConfiguredTableAssociation",
"cleanrooms:GetMembership",
"cleanrooms:GetProtectedQuery",
"cleanrooms:GetSchema",
"cleanrooms:GetSchemaAnalysisRule",
"cleanrooms:ListAnalysisTemplates",
"cleanrooms:ListCollaborationAnalysisTemplates",
"cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
"cleanrooms:ListCollaborations",
"cleanrooms:ListConfiguredTableAssociations",
"cleanrooms:ListConfiguredTables",
"cleanrooms:ListMembers",
"cleanrooms:ListMemberships",
"cleanrooms:ListProtectedQueries",
"cleanrooms:ListSchemas",
"cleanrooms:ListTagsForResource",
"cleanrooms-ml:GetTrainingDataset",
"cleanrooms-ml:GetAudienceGenerationJob",
"cleanrooms-ml:GetAudienceModel",
"cleanrooms-ml:GetConfiguredAudienceModel",
"cleanrooms-ml:GetConfiguredAudienceModelPolicy",
"cleanrooms-ml:ListAudienceExportJobs",
"cleanrooms-ml:ListAudienceGenerationJobs",
"cleanrooms-ml:ListAudienceModels",
"cleanrooms-ml:ListConfiguredAudienceModels",
"cleanrooms-ml:ListTrainingDatasets",
"cleanrooms-ml: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",
"deadline:BatchGetJobEntity",
"deadline:GetApplicationVersion",
"deadline:GetBudget",
"deadline:GetFarm",
"deadline:GetFleet",
"deadline:GetJob",
"deadline:GetLicenseEndpoint",
"deadline:GetMonitor",
"deadline:GetQueue",
"deadline:GetQueueEnvironment",
"deadline:GetQueueFleetAssociation",
"deadline:GetSession",
"deadline:GetSessionAction",
"deadline:GetSessionsStatisticsAggregation",
"deadline:GetStep",
"deadline:GetStorageProfile",
"deadline:GetStorageProfileForQueue",
"deadline:GetTask",
"deadline:GetWorker",
"deadline:ListAvailableMeteredProducts",
"deadline:ListBudgets",
"deadline:ListFarmMembers",
"deadline:ListFarms",
"deadline:ListFleetMembers",
"deadline:ListFleets",
"deadline:ListJobMembers",
"deadline:ListJobs",
"deadline:ListLicenseEndpoints",
"deadline:ListMeteredProducts",
"deadline:ListMonitors",
"deadline:ListQueueEnvironments",
"deadline:ListQueueFleetAssociations",
"deadline:ListQueueMembers",
"deadline:ListQueues",
"deadline:ListSessionActions",
"deadline:ListSessions",
```

```
"deadline:ListSessionsForWorker",
"deadline:ListStepConsumers",
"deadline:ListStepDependencies",
"deadline:ListSteps",
"deadline:ListStorageProfiles",
"deadline:ListStorageProfilesForQueue",
"deadline:ListTagsForResource",
"deadline:ListTasks",
"deadline:ListWorkers",
"deadline:SearchJobs",
"deadline:SearchSteps",
"deadline:SearchTasks",
"deadline:SearchWorkers",
"deepcomposer:GetComposition",
"deepcomposer:GetModel",
"deepcomposer:GetSampleModel",
"deepcomposer:ListCompositions",
"deepcomposer:ListModels",
"deepcomposer:ListSampleModels",
"deepcomposer:ListTrainingTopics",
"detective:BatchGetGraphMemberDatasources",
"detective:BatchGetMembershipDatasources",
"detective:Get*",
"detective:List*",
"detective:SearchGraph",
"devicefarm:Get*",
"devicefarm:List*",
"devops-guru:DescribeAccountHealth",
"devops-guru:DescribeAccountOverview",
"devops-guru:DescribeAnomaly",
"devops-guru:DescribeEventSourcesConfig",
"devops-guru:DescribeFeedback",
"devops-guru:DescribeInsight",
"devops-guru:DescribeOrganizationHealth",
"devops-guru:DescribeOrganizationOverview",
"devops-guru:DescribeOrganizationResourceCollectionHealth",
"devops-guru:DescribeResourceCollectionHealth",
"devops-guru:DescribeServiceIntegration",
"devops-guru:GetCostEstimation",
"devops-guru:GetResourceCollection",
"devops-guru:ListAnomaliesForInsight",
"devops-guru:ListAnomalousLogGroups",
"devops-guru:ListEvents",
"devops-guru:ListInsights",
```

```
"devops-guru:ListMonitoredResources",
"devops-guru:ListNotificationChannels",
"devops-guru:ListOrganizationInsights",
"devops-guru:ListRecommendations",
"devops-guru:SearchInsights",
"devops-guru:StartCostEstimation",
"directconnect:Describe*",
"discovery:Describe*",
"discovery:Get*",
"discovery:List*",
"dlm:Get*",
"dms:Describe*",
"dms:List*",
"dms:Test*",
"drs:DescribeJobLogItems",
"drs:DescribeJobs",
"drs:DescribeLaunchConfigurationTemplates",
"drs:DescribeRecoveryInstances",
"drs:DescribeRecoverySnapshots",
"drs:DescribeReplicationConfigurationTemplates",
"drs:DescribeSourceNetworks",
"drs:DescribeSourceServers",
"drs:GetFailbackReplicationConfiguration",
"drs:GetLaunchConfiguration",
"drs:GetReplicationConfiguration",
"drs:ListExtensibleSourceServers",
"drs:ListLaunchActions",
"drs:ListStagingAccounts",
"drs:ListTagsForResource",
"ds:Check*",
"ds:Describe*",
"ds:Get*",
"ds:List*",
"ds:Verify*",
"dynamodb:BatchGet*",
"dynamodb:Describe*",
"dynamodb:Get*",
"dynamodb:List*",
"dynamodb: PartiQLSelect",
"dynamodb:Query",
"dynamodb:Scan",
"ec2:Describe*",
"ec2:Get*",
"ec2:ListImagesInRecycleBin",
```

```
"ec2:ListSnapshotsInRecycleBin",
"ec2:SearchLocalGatewayRoutes",
"ec2:SearchTransitGatewayRoutes",
"ec2messages:Get*",
"ecr-public:BatchCheckLayerAvailability",
"ecr-public:DescribeImages",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetAuthorizationToken",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchCheck*",
"ecr:BatchGet*",
"ecr:Describe*",
"ecr:Get*",
"ecr:List*",
"ecs:Describe*",
"ecs:List*",
"eks:Describe*",
"eks:List*",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:DescribeAccelerators",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:ListTagsForResource",
"elasticache:Describe*",
"elasticache:List*",
"elasticbeanstalk:Check*",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
"elasticbeanstalk:Request*",
"elasticbeanstalk:Retrieve*",
"elasticbeanstalk:Validate*",
"elasticfilesystem:Describe*",
"elasticfilesystem:ListTagsForResource",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:List*",
"elasticmapreduce:View*",
"elastictranscoder:List*",
"elastictranscoder:Read*",
```

```
"elemental-appliances-software:Get*",
"elemental-appliances-software:List*",
"emr-containers:DescribeJobRun",
"emr-containers:DescribeManagedEndpoint",
"emr-containers:DescribeVirtualCluster",
"emr-containers:ListJobRuns",
"emr-containers:ListManagedEndpoints",
"emr-containers:ListTagsForResource",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
"emr-serverless:GetDashboardForJobRun",
"emr-serverless:GetJobRun",
"emr-serverless:ListApplications",
"emr-serverless:ListJobRuns",
"emr-serverless:ListTagsForResource",
"es:Describe*",
"es:ESHttpGet",
"es:ESHttpHead",
"es:Get*",
"es:List*",
"events:Describe*",
"events:List*",
"events:Test*",
"evidently:GetExperiment",
"evidently:GetExperimentResults",
"evidently:GetFeature",
"evidently:GetLaunch",
"evidently:GetProject",
"evidently:GetSegment",
"evidently:ListExperiments",
"evidently:ListFeatures",
"evidently:ListLaunches",
"evidently:ListProjects",
"evidently:ListSegmentReferences",
"evidently:ListSegments",
"evidently:ListTagsForResource",
"evidently:TestSegmentPattern",
"firehose:Describe*",
"firehose:List*",
"fis:GetAction",
"fis:GetExperiment",
"fis:GetExperimentTargetAccountConfiguration",
"fis:GetExperimentTemplate",
"fis:GetTargetAccountConfiguration",
```

```
"fis:GetTargetResourceType",
"fis:ListActions",
"fis:ListExperimentResolvedTargets",
"fis:ListExperiments",
"fis:ListExperimentTargetAccountConfigurations",
"fis:ListExperimentTemplates",
"fis:ListTagsForResource",
"fis:ListTargetAccountConfigurations",
"fis:ListTargetResourceTypes",
"fms:GetAdminAccount",
"fms:GetAppsList",
"fms:GetComplianceDetail",
"fms:GetNotificationChannel",
"fms:GetPolicy",
"fms:GetProtectionStatus",
"fms:GetProtocolsList",
"fms:GetViolationDetails",
"fms:ListAppsLists",
"fms:ListComplianceStatus",
"fms:ListMemberAccounts",
"fms:ListPolicies",
"fms:ListProtocolsLists",
"fms:ListTagsForResource",
"forecast:DescribeAutoPredictor",
"forecast:DescribeDataset",
"forecast:DescribeDatasetGroup",
"forecast:DescribeDatasetImportJob",
"forecast:DescribeExplainability",
"forecast:DescribeExplainabilityExport",
"forecast:DescribeForecast",
"forecast:DescribeForecastExportJob",
"forecast:DescribeMonitor",
"forecast:DescribePredictor",
"forecast:DescribePredictorBacktestExportJob",
"forecast:DescribeWhatIfAnalysis",
"forecast:DescribeWhatIfForecast",
"forecast:DescribeWhatIfForecastExport",
"forecast:GetAccuracyMetrics",
"forecast:ListDatasetGroups",
"forecast:ListDatasetImportJobs",
"forecast:ListDatasets",
"forecast:ListExplainabilities",
"forecast:ListExplainabilityExports",
"forecast:ListForecastExportJobs",
```



```
"forecast:ListForecasts",
"forecast:ListMonitorEvaluations",
"forecast:ListMonitors",
"forecast:ListPredictorBacktestExportJobs",
"forecast:ListPredictors",
"forecast:ListWhatIfAnalyses",
"forecast:ListWhatIfForecastExports",
"forecast:ListWhatIfForecasts",
"forecast:QueryForecast",
"forecast:QueryWhatIfForecast",
"frauddetector:BatchGetVariable",
"frauddetector:DescribeDetector",
"frauddetector:DescribeModelVersions",
"frauddetector:GetBatchImportJobs",
"frauddetector:GetBatchPredictionJobs",
"frauddetector:GetDeleteEventsByEventTypeStatus",
"frauddetector:GetDetectors",
"frauddetector:GetDetectorVersion",
"frauddetector:GetEntityTypes",
"frauddetector:GetEvent",
"frauddetector:GetEventPredictionMetadata",
"frauddetector:GetEventTypes",
"frauddetector:GetExternalModels",
"frauddetector:GetKMSEncryptionKey",
"frauddetector:GetLabels",
"frauddetector:GetListElements",
"frauddetector:GetListsMetadata",
"frauddetector:GetModels",
"frauddetector:GetModelVersion",
"frauddetector:GetOutcomes",
"frauddetector:GetRules",
"frauddetector:GetVariables",
"frauddetector:ListEventPredictions",
"frauddetector:ListTagsForResource",
"freertos:Describe*",
"freertos:List*",
"freetier:GetFreeTierAlertPreference",
"freetier:GetFreeTierUsage",
"fsx:Describe*",
"fsx:List*",
"gamelift:Describe*",
"gamelift:Get*",
"gamelift:List*",
"gamelift:ResolveAlias",
```

```
"gamelift:Search*",
"glacier:Describe*",
"glacier:Get*",
"glacier:List*",
"globalaccelerator:Describe*",
"globalaccelerator:List*",
"glue:BatchGetCrawlers",
"glue:BatchGetDevEndpoints",
"glue:BatchGetJobs",
"glue:BatchGetPartition",
"glue:BatchGetTriggers",
"glue:BatchGetWorkflows",
"glue:CheckSchemaVersionValidity",
"glue:GetCatalogImportStatus",
"glue:GetClassifier",
"glue:GetClassifiers",
"glue:GetCrawler",
"glue:GetCrawlerMetrics",
"glue:GetCrawlers",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDataflowGraph",
"glue:GetDevEndpoint",
"glue:GetDevEndpoints",
"glue:GetJob",
"glue:GetJobBookmark",
"glue:GetJobRun",
"glue:GetJobRuns",
"glue:GetJobs",
"glue:GetMapping",
"glue:GetMLTaskRun",
"glue:GetMLTaskRuns",
"glue:GetMLTransform",
"glue:GetMLTransforms",
"glue:GetPartition",
"glue:GetPartitions",
"glue:GetPlan",
"glue:GetRegistry",
"glue:GetResourcePolicy",
"glue:GetSchema",
"glue:GetSchemaByDefinition",
"glue:GetSchemaVersion",
"glue:GetSchemaVersionsDiff",
```

```
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTables",
"glue:GetTableVersion",
"glue:GetTableVersions",
"glue:GetTags",
"glue:GetTrigger",
"glue:GetTriggers",
"glue:GetUserDefinedFunction",
"glue:GetUserDefinedFunctions",
"glue:GetWorkflow",
"glue:GetWorkflowRun",
"glue:GetWorkflowRunProperties",
"glue:GetWorkflowRuns",
"glue:ListCrawlers",
"glue:ListCrawls",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
"glue:ListRegistries",
"glue:ListSchemas",
"glue:ListSchemaVersions",
"glue:ListTriggers",
"glue:ListWorkflows",
"glue:QuerySchemaVersionMetadata",
"glue:SearchTables",
"grafana:DescribeWorkspace",
"grafana:DescribeWorkspaceAuthentication",
"grafana:DescribeWorkspaceConfiguration",
"grafana:ListPermissions",
"grafana:ListTagsForResource",
"grafana:ListVersions",
"grafana:ListWorkspaces",
"greengrass:DescribeComponent",
"greengrass:Get*",
"greengrass:List*",
"groundstation:DescribeContact",
"groundstation:GetConfig",
"groundstation:GetDataflowEndpointGroup",
"groundstation:GetMinuteUsage",
"groundstation:GetMissionProfile",
"groundstation:GetSatellite",
"groundstation:ListConfigs",
```

```
"groundstation:ListContacts",
"groundstation:ListDataflowEndpointGroups",
"groundstation:ListGroundStations",
"groundstation:ListMissionProfiles",
"groundstation:ListSatellites",
"groundstation:ListTagsForResource",
"guardduty:Describe*",
"guardduty:Get*",
"guardduty:List*",
"health:Describe*",
"healthlake:DescribeFHIRDatastore",
"healthlake:DescribeFHIRExportJob",
"healthlake:DescribeFHIRImportJob",
"healthlake:GetCapabilities",
"healthlake:ListFHIRDatastores",
"healthlake:ListFHIRExportJobs",
"healthlake:ListFHIRImportJobs",
"healthlake:ListTagsForResource",
"healthlake:ReadResource",
"healthlake:SearchWithGet",
"healthlake:SearchWithPost",
"iam:Generate*",
"iam:Get*",
"iam:List*",
"iam:Simulate*",
"identity-sync:GetSyncProfile",
"identity-sync:GetSyncTarget",
"identity-sync:ListSyncFilters",
"identitystore-auth:BatchGetSession",
"identitystore-auth:ListSessions",
"identitystore:DescribeGroup",
"identitystore:DescribeGroupMembership",
"identitystore:DescribeUser",
"identitystore:GetGroupId",
"identitystore:GetGroupMembershipId",
"identitystore:GetUserId",
"identitystore:IsMemberInGroups",
"identitystore:ListGroupMemberships",
"identitystore:ListGroupMembershipsForMember",
"identitystore:ListGroups",
"identitystore:ListUsers",
"imagebuilder:Get*",
"imagebuilder:List*",
"importexport:Get*",
```

```
"importexport:List*",
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
"inspector2:BatchGetAccountStatus",
"inspector2:BatchGetFreeTrialInfo",
"inspector2:DescribeOrganizationConfiguration",
"inspector2:GetDelegatedAdminAccount",
"inspector2:GetFindingsReportStatus",
"inspector2:GetMember",
"inspector2:ListAccountPermissions",
"inspector2:ListCisScans",
"inspector2:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListMembers",
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"internetmonitor:GetHealthEvent",
"internetmonitor:GetInternetEvent",
"internetmonitor:GetMonitor",
"internetmonitor:ListHealthEvents",
"internetmonitor:ListInternetEvents",
"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:GetMetrics",
"iotwireless:GetMetricConfiguration",
"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:GetComposition",
"ivs:GetEncoderConfiguration",
"ivs:GetStage",
"ivs:GetStageSession",
"ivs:GetParticipant",
"ivs:GetPlaybackKeyPair",
"ivs:GetPlaybackRestrictionPolicy",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamSession",
"ivs:ListChannels",
"ivs:ListCompositions",
"ivs:ListEncoderConfigurations",
"ivs:ListParticipants",
"ivs:ListParticipantEvents",
"ivs:ListPlaybackKeyPairs",
"ivs:ListPlaybackRestrictionPolicies",
"ivs:ListRecordingConfigurations",
"ivs:ListStages",
"ivs:ListStageSessions",
"ivs:ListStreams",
"ivs:ListStreamKeys",
"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:GetCloudWatchAlarmTemplate",
"medialive:GetCloudWatchAlarmTemplateGroup",
"medialive:GetEventBridgeRuleTemplate",
"medialive:GetEventBridgeRuleTemplateGroup",
"medialive:GetSignalMap",
"medialive:ListChannels",
"medialive:ListCloudWatchAlarmTemplateGroups",
"medialive:ListCloudWatchAlarmTemplates",
"medialive:ListEventBridgeRuleTemplateGroups",
"medialive:ListEventBridgeRuleTemplates",
"medialive:ListInputDevices",
"medialive:ListInputDeviceTransfers",
"medialive:ListInputs",
"medialive:ListInputSecurityGroups",
"medialive:ListMultiplexes",
"medialive:ListMultiplexPrograms",
"medialive:ListOfferings",
"medialive:ListReservations",
"medialive:ListSignalMaps",
"medialive:ListTagsForResource",
"mediapackage-vod:Describe*",
"mediapackage-vod:List*",
"mediapackage:Describe*",
"mediapackage:List*",
"mediapackagev2:GetChannel",
"mediapackagev2:GetChannelGroup",
"mediapackagev2:GetChannelPolicy",
"mediapackagev2:GetHeadObject",
"mediapackagev2:GetObject",
"mediapackagev2:GetOriginEndpoint",
"mediapackagev2:GetOriginEndpointPolicy",
"mediapackagev2:ListChannelGroups",
"mediapackagev2:ListChannels",
"mediapackagev2:ListOriginEndpoints",
"mediapackagev2:ListTagsForResource",
"mediastore:DescribeContainer",
```



```
"mediastore:DescribeObject",
"mediastore:GetContainerPolicy",
"mediastore:GetCorsPolicy",
"mediastore:GetLifecyclePolicy",
"mediastore:GetMetricPolicy",
"mediastore:GetObject",
"mediastore:ListContainers",
"mediastore:ListItems",
"mediastore:ListTagsForResource",
"memorydb: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-serverless:GetCustomDomainAssociation",
"redshift-serverless:GetEndpointAccess",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetRecoveryPoint",
"redshift-serverless:GetResourcePolicy",
"redshift-serverless:GetScheduledAction",
"redshift-serverless:GetSnapshot",
"redshift-serverless:GetTableRestoreStatus",
"redshift-serverless:GetUsageLimit",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:ListCustomDomainAssociations",
"redshift-serverless:ListEndpointAccess",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListRecoveryPoints",
"redshift-serverless:ListScheduledActions",
"redshift-serverless:ListSnapshotCopyConfigurations",
"redshift-serverless:ListSnapshots",
"redshift-serverless:ListTableRestoreStatus",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListUsageLimits",
"redshift-serverless:ListWorkgroups",
"redshift:Describe*",
"redshift:GetReservedNodeExchangeOfferings",
"redshift:ListRecommendations",
"redshift:View*",
"refactor-spaces:GetApplication",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetResourcePolicy",
"refactor-spaces:GetRoute",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces: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*",
"route53profiles:GetProfile",
"route53profiles:GetProfileAssociation",
"route53profiles:GetProfileResourceAssociation",
"route53profiles:ListProfileAssociations",
"route53profiles:ListProfileResourceAssociations",
"route53profiles:ListProfiles",
"route53profiles:ListTagsForResource",
"route53resolver:Get*",
"route53resolver:List*",
"rum:GetAppMonitor",
"rum:GetAppMonitorData",
"rum:ListAppMonitors",
"s3-object-lambda:GetObject",
"s3-object-lambda:GetObjectAcl",
"s3-object-lambda:GetObjectLegalHold",
```



```
"s3-object-lambda:GetObjectRetention",
"s3-object-lambda:GetObjectTagging",
"s3-object-lambda:GetObjectVersion",
"s3-object-lambda:GetObjectVersionAcl",
"s3-object-lambda:GetObjectVersionTagging",
"s3-object-lambda:ListBucket",
"s3-object-lambda:ListBucketMultipartUploads",
"s3-object-lambda:ListBucketVersions",
"s3-object-lambda:ListMultipartUploadParts",
"s3: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*",
"securitylake:GetDataLakeExceptionSubscription",
"securitylake:GetDataLakeOrganizationConfiguration",
"securitylake:GetDataLakeSources",
"securitylake:GetSubscriber",
"securitylake:ListDataLakeExceptions",
"securitylake:ListDataLakes",
"securitylake:ListLogSources",
"securitylake:ListSubscribers",
"securitylake:ListTagsForResource",
"serverlessrepo:Get*",
"serverlessrepo:List*",
"serverlessrepo:SearchApplications",
"servicecatalog:Describe*",
"servicecatalog:GetApplication",
"servicecatalog:GetAttributeGroup",
"servicecatalog:List*",
"servicecatalog:Scan*",
"servicecatalog:Search*",
"servicediscovery:DiscoverInstances",
"servicediscovery:DiscoverInstancesRevision",
"servicediscovery:Get*",
"servicediscovery:List*",
"servicequotas: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",
"signin:ListTrustedIdentityPropagationApplicationsForConsole",
"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*",
"states:ValidateStateMachineDefinition",
"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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ResourceGroupsandTagEditorFullAccess

Descrizione: Fornisce l'accesso completo a Resource Groups e Tag Editor.

ResourceGroupsandTagEditorFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ResourceGroupsandTagEditorFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC

- Ora modificata: 10 agosto 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)

- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ResourceGroupsandTagEditorReadOnlyAccess

Descrizione: Fornisce l'accesso all'utilizzo di Resource Groups e Tag Editor, ma non consente la modifica dei tag tramite il Tag Editor.

ResourceGroupsandTagEditorReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ResourceGroupsandTagEditorReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 10 agosto 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ResourceGroupsServiceRolePolicy

Descrizione: consente ai AWS Resource Groups di interrogare i AWS servizi che possiedono le tue risorse per mantenere il gruppo up-to-date

ResourceGroupsServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 5 gennaio 2023, 16:57 UTC
- Ora modificata: 05 gennaio 2023, 16:57 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

Descrizione: consente all'operatore del driver OpenShift Amazon EBS Container Storage Interface (CSI) di installare e gestire il driver Amazon EBS CSI su un cluster Red Hat OpenShift Service on AWS (ROSA). Il driver Amazon EBS CSI consente ai cluster ROSA di gestire il ciclo di vita dei volumi Amazon EBS per volumi persistenti.

R0SAAmazonEBSCSIDriverOperatorPolicy è una politica gestita.AWS

Utilizzo di questa politica

Puoi collegarti R0SAAmazonEBSCSIDriverOperatorPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 22:36 UTC
- Ora modificata: 20 aprile 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/R0SAAmazonEBSCSIDriverOperatorPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    ]
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSACloudNetworkConfigOperatorPolicy

Descrizione: Consente all'operatore del OpenShift Cloud Network Config Controller di fornire e gestire le risorse di rete per l'utilizzo da parte dell'overlay di rete del cluster Red Hat OpenShift Service on AWS (ROSA). Il OpenShift Cloud Network Operator si interfaccia con le AWS API per conto dei plugin di rete tramite CustomResourceDefinitions. L'operatore utilizza queste autorizzazioni di policy per gestire gli indirizzi IP privati per le istanze Amazon EC2 come parte del cluster ROSA.

ROSACloudNetworkConfigOperatorPolicy è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti ROSACloudNetworkConfigOperatorPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 22:34 UTC
- Ora modificata: 20 aprile 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAControlPlaneOperatorPolicy

Descrizione: consente al piano di controllo Red Hat OpenShift Service on AWS (ROSA) di gestire le risorse del cluster ROSA Amazon EC2 e Amazon Route 53.

ROSAControlPlaneOperatorPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ROSAControlPlaneOperatorPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 aprile 2023, 23:02 UTC
- Ora modificata: 30 giugno 2023, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAImageRegistryOperatorPolicy

Descrizione: consente all' OpenShift Image Registry Operator di effettuare il provisioning e la gestione di bucket e oggetti Amazon S3 per l'utilizzo da parte del registro di immagini interno al cluster Red Hat OpenShift Service on AWS (ROSA) per soddisfare i requisiti di storage ROSA. L' OpenShift Image Registry Operator installa e gestisce il registro interno di un cluster Red Hat. OpenShift

ROSAImageRegistryOperatorPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti `R0SAImageRegistryOperatorPolicy` ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 aprile 2023, 20:13 UTC
- Ora modificata: 12 dicembre 2023, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/R0SAImageRegistryOperatorPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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}/*"
    ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAIngressOperatorPolicy

Descrizione: Consente all'operatore OpenShift Ingress di fornire e gestire sistemi di bilanciamento del carico e configurazioni DNS (Domain Name System) per i cluster Red Hat OpenShift Service on AWS (ROSA). La policy consente l'accesso in lettura ai valori dei tag, che l'operatore filtra per le risorse Route 53 per scoprire le zone ospitate.

ROSAIngressOperatorPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ROSAIngressOperatorPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 22:37 UTC
- Ora modificata: 20 aprile 2023, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        ]
      }
    }
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAInstallerPolicy

Descrizione: Consente al programma di installazione di Red Hat OpenShift Service on AWS (ROSA) di gestire AWS le risorse che supportano l'installazione del cluster ROSA. Ciò include la gestione dei profili di istanza per i nodi di lavoro ROSA.

ROSAInstallerPolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ROSAInstallerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 giugno 2023, 21:00 UTC
- Ora modificata: 24 aprile 2024, 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",

```

```

        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
},
{
    "Sid" : "PassRoleToEC2",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:*:iam:*:role/*-ROSA-Worker-Role"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "ec2.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "ManageInstanceProfiles",
    "Effect" : "Allow",
    "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:GetInstanceProfile"
    ],
    "Resource" : [
        "arn:aws:iam:*:instance-profile/rosa-service-managed-*"
    ]
},
{
    "Sid" : "CreateInstanceProfiles",
    "Effect" : "Allow",
    "Action" : [

```

```

        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
    ],
    "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "GetSecretValue",
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:GetSecretValue"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "Route53ManageRecords",
    "Effect" : "Allow",
    "Action" : [
        "route53:ChangeResourceRecordSets"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAllValues:StringLike" : {
            "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
                "*.openshiftapps.com",
                "*.devshift.org",
                "*.hypershift.local",
                "*.openshiftusgov.com",
                "*.devshiftusgov.com"
            ]
        }
    }
}

```

```

    }
  },
  {
    "Sid" : "Route53Manage",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeTagsForResource",
      "route53:CreateHostedZone",
      "route53>DeleteHostedZone"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CreateTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "RunInstances"
        ]
      }
    }
  },
  {
    "Sid" : "RunInstancesNoCondition",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:snapshot/*"
    ]
  },
  {
    "Sid" : "RunInstancesRestrictedRequestTag",
    "Effect" : "Allow",

```

```

    "Action" : "ec2:RunInstances",
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "RunInstancesRedHatOwnedAMIs",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:image/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ec2:Owner" : [
                "531415883065",
                "251351625822",
                "210686502322"
            ]
        }
    }
},
{
    "Sid" : "ManageInstancesRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},

```



```
{
  "Sid" : "CreateGrantRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : "ec2.*.amazonaws.com"
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    }
  }
},
{
  "Sid" : "ManagedKMSRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group*/*"
  ],
  "Condition" : {
    "StringEquals" : {
```

```
        "aws:RequestTag/red-hat-managed" : "true"
    }
}
},
{
    "Sid" : "DeleteSecurityGroup",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteSecurityGroup"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:security-group/*/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "SecurityGroupIngressEgress",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:security-group/*/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "CreateSecurityGroupsVPCNoCondition",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
```

```

        "arn:aws:ec2:*:*:vpc/*"
    ],
},
{
    "Sid" : "CreateTagsRestrictedActions",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ec2:CreateAction" : [
                "CreateSecurityGroup"
            ]
        }
    }
},
{
    "Sid" : "CreateTagsK8sSubnet",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
    ],
    "Condition" : {
        "ForAllValues:StringLike" : {
            "aws:TagKeys" : [
                "kubernetes.io/cluster/*"
            ]
        }
    }
},
{
    "Sid" : "ListPoliciesAttachedToRoles",
    "Effect" : "Allow",
    "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
    ],

```

```
"Resource" : "arn:aws:iam::*:role/*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/red-hat-managed" : "true"
  }
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAKMSPProviderPolicy

Descrizione: consente al ROSA AWS Encryption Provider integrato di gestire le AWS chiavi KMS (Key Management Service) per supportare la crittografia dei dati etcd utilizzando una chiave AWS KMS fornita dal cliente. La politica consente la crittografia e la decrittografia dei dati utilizzando le chiavi KMS.

ROSAKMSPProviderPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti ROSAKMSPProviderPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 aprile 2023, 20:10 UTC
- Ora modificata: 27 aprile 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSPProviderPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAKubeControllerPolicy

Descrizione: consente al controller ROSA Kubernetes di gestire le risorse Amazon EC2, Elastic Load Balancing (ELB) e AWS Key Management Service (KMS) per un cluster ROSA.

ROSAKubeControllerPolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti ROSAKubeControllerPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 aprile 2023, 20:09 UTC
- Ora modificata: 16 ottobre 2023, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
    }
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAManageSubscription

Descrizione: Questa policy fornisce le autorizzazioni necessarie per gestire la sottoscrizione Red Hat OpenShift Service on AWS (ROSA).

ROSAManageSubscription è una [policy AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ROSAManageSubscription ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 11 aprile 2022, 20:58 UTC
- Ora modificata: 04 agosto 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSANodePoolManagementPolicy

Descrizione: consente a Red Hat OpenShift Service on AWS (ROSA) di gestire le istanze EC2 del cluster come nodi di lavoro, inclusa l'autorizzazione a configurare gruppi di sicurezza e etichettare istanze e volumi. Questa policy consente anche l'uso di istanze EC2 con crittografia del disco fornita dalle AWS chiavi del Key Management Service (KMS).

R0SANodePoolManagementPolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti R0SANodePoolManagementPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 08 giugno 2023, 20:48 UTC
- Ora modificata: 2 maggio 2024, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/R0SANodePoolManagementPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:*:iam:*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
    ],
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
    }
},
{
    "Sid" : "PassWorkerRole",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:*:iam:*:role/*-ROSA-Worker-Role"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : [
                "ec2.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
    ],

```

```
"Resource" : [
  "arn:aws:ec2:*:*:security-group/*",
  "arn:aws:ec2:*:*:security-group-rule/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/red-hat-managed" : "true"
  }
}
},
{
  "Sid" : "NetworkInterfaces",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "NetworkInterfacesNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:vpc/*"
  ]
},
{
  "Sid" : "TerminateInstances",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : [
```

```

        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "CreateTags",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
    ],
    "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"
    }
  }
}
```

```
}  
  }  
    }  
  ]  
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSASRESupportPolicy

Descrizione: Fornisce a ROSA Site Reliability Engineering (SRE) le autorizzazioni necessarie per osservare, diagnosticare e supportare inizialmente AWS le risorse associate a Red Hat OpenShift Service on AWS (ROSA) sui cluster, inclusa la possibilità di modificare lo stato del nodo del cluster ROSA.

ROSASRESupportPolicy [è una policy gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti ROSASRESupportPolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 giugno 2023, 14:36 UTC
- Ora modificata: 10 aprile 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:iam:*:*:instance-profile/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "DescribeSpotFleetInstances",
    "Effect" : "Allow",
    "Action" : "ec2:DescribeSpotFleetInstances",
    "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",

```

```
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageInstanceLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ROSAWorkerInstancePolicy

Descrizione: consente ai nodi di lavoro Red Hat OpenShift Service on AWS (ROSA) del tuo account l'accesso in sola lettura alle istanze Amazon EC2 Regioni AWS e per la gestione del ciclo di vita dei nodi di calcolo.

ROSAWorkerInstancePolicy è [una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti ROSAWorkerInstancePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 22:35 UTC
- Ora modificata: 20 aprile 2023, 22:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ]
    }
  ]
}
```

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

Route53RecoveryReadinessServiceRolePolicy

Descrizione: policy Service Linked Role per la preparazione al ripristino della Route 53

Route53RecoveryReadinessServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 15 luglio 2021, 16:06 UTC
- Ora modificata: 14 febbraio 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}

```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

Route53ResolverServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Route53 Resolver

Route53ResolverServiceRolePolicy [è una politica gestita AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 12 agosto 2020, 17:47 UTC
- Ora modificata: 12 agosto 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

S3StorageLensServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da S3 Storage Lens

S3StorageLensServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 18 novembre 2020, 18:15 UTC
- Ora modificata: 18 novembre 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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



```
"Statement" : [
  {
    "Sid" : "AwsOrgsAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeOrganization",
      "organizations:ListAccounts",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

SecretsManagerReadWrite

Descrizione: fornisce l'accesso in lettura/scrittura a AWS Secrets Manager tramite. AWS Management Console Nota: questo esclude le azioni IAM, quindi combinalo con IAM FullAccess se è richiesta la configurazione di rotazione.

SecretsManagerReadWrite è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti SecretsManagerReadWrite ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 4 aprile 2018, 18:05 UTC
- Ora modificata: 22 febbraio 2024, 18:12 UTC

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

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ],
  "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-*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

SecurityAudit

Descrizione: il modello di controllo di sicurezza consente l'accesso alla lettura dei metadati di configurazione di sicurezza. È utile per i software che controllano la configurazione di un Account AWS

SecurityAudit è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti SecurityAudit ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 5 aprile 2024, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Versione della politica

Versione della politica: v42 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
```

```
"access-analyzer:GetFinding",
"access-analyzer:ListAnalyzedResources",
"access-analyzer:ListAnalyzers",
"access-analyzer:ListArchiveRules",
"access-analyzer:ListFindings",
"access-analyzer:ListTagsForResource",
"account:GetAlternateContact",
"account:GetRegionOptStatus",
"acm-pca:DescribeCertificateAuthority",
"acm-pca:DescribeCertificateAuthorityAuditReport",
"acm-pca:GetPolicy",
"acm-pca:ListCertificateAuthorities",
"acm-pca:ListPermissions",
"acm-pca:ListTags",
"acm:Describe*",
"acm:List*",
"airflow:GetEnvironment",
"airflow:ListEnvironments",
"appflow:ListFlows",
"appflow:ListTagsForResource",
"application-autoscaling:Describe*",
"appmesh:Describe*",
"appmesh:List*",
"apprunner:DescribeAutoScalingConfiguration",
"apprunner:DescribeCustomDomains",
"apprunner:DescribeObservabilityConfiguration",
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
"apprunner:DescribeVpcIngressConnection",
"apprunner:ListAutoScalingConfigurations",
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appsync:GetApiCache",
"appsync:List*",
"athena:GetWorkGroup",
"athena:List*",
"auditmanager:GetAccountStatus",
"auditmanager:ListAssessmentControlInsightsByControlDomain",
"auditmanager:ListAssessmentFrameworkShareRequests",
```

```
"auditmanager:ListAssessmentFrameworks",
"auditmanager:ListAssessmentReports",
"auditmanager:ListAssessments",
"auditmanager:ListControlDomainInsights",
"auditmanager:ListControlDomainInsightsByAssessment",
"auditmanager:ListControlInsightsByControlDomain",
"auditmanager:ListControls",
"auditmanager:ListNotifications",
"auditmanager:ListTagsForResource",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling:Describe*",
"backup:DescribeGlobalSettings",
"backup:DescribeRegionSettings",
"backup:GetBackupVaultAccessPolicy",
"backup:GetBackupVaultNotifications",
"backup:ListBackupVaults",
"backup:ListTags",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobDefinitions",
"bedrock:GetCustomModel",
"bedrock:GetModelInvocationLoggingConfiguration",
"bedrock:ListCustomModels",
"bedrock:ListTagsForResource",
"braket:SearchJobs",
"braket:SearchQuantumTasks",
"chime:List*",
"cloud9:Describe*",
"cloud9:ListEnvironments",
"clouddirectory:ListDirectories",
"cloudformation:DescribeStack*",
"cloudformation:GetStackPolicy",
"cloudformation:GetTemplate",
"cloudformation:ListStack*",
"cloudfront:Get*",
"cloudfront:List*",
"cloudsearch:DescribeDomainEndpointOptions",
"cloudsearch:DescribeDomains",
"cloudsearch:DescribeServiceAccessPolicies",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetInsightSelectors",
"cloudtrail:GetTrail",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
```

```
"cloudtrail:ListTrails",
"cloudtrail:LookupEvents",
"cloudwatch:Describe*",
"cloudwatch:GetDashboard",
"cloudwatch:ListDashboards",
"cloudwatch:ListTagsForResource",
"codeartifact:GetDomainPermissionsPolicy",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListRepositories",
"codebuild:BatchGetProjects",
"codebuild:GetResourcePolicy",
"codebuild:ListProjects",
"codecommit:BatchGetRepositories",
"codecommit:GetBranch",
"codecommit:GetObjectIdentifier",
"codecommit:GetRepository",
"codecommit:GetRepositoryTriggers",
"codecommit:List*",
"codedeploy:Batch*",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:GetJobDetails",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineExecution",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"codestar:Describe*",
"codestar:List*",
"cognito-identity:Describe*",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:ListIdentityPools",
"cognito-identity:ListTagsForResource",
"cognito-idp:Describe*",
"cognito-idp:ListDevices",
"cognito-idp:ListGroups",
"cognito-idp:ListIdentityProviders",
"cognito-idp:ListResourceServers",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserImportJobs",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListUserPools",
"cognito-idp:ListUsers",
"cognito-idp:ListUsersInGroup",
"cognito-sync:Describe*",
```

```
"cognito-sync:List*",
"comprehend:Describe*",
"comprehend:List*",
"comprehendmedical:ListICD10CMInferenceJobs",
"comprehendmedical:ListPHIDetectionJobs",
"comprehendmedical:ListRxNormInferenceJobs",
"comprehendmedical:ListSNOMEDCTInferenceJobs",
"config:BatchGetAggregateResourceConfig",
"config:BatchGetResourceConfig",
"config:Deliver*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:SelectAggregateResourceConfig",
"config:SelectResourceConfig",
"connect:ListApprovedOrigins",
"connect:ListInstanceAttributes",
"connect:ListInstanceStorageConfigs",
"connect:ListInstances",
"connect:ListIntegrationAssociations",
"connect:ListLambdaFunctions",
"connect:ListLexBots",
"connect:ListSecurityKeys",
"databrew:DescribeDataset",
"databrew:DescribeProject",
"databrew:ListJobs",
"databrew:ListProjects",
"dataexchange:ListDataSets",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:EvaluateExpression",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:QueryObjects",
"datapipeline:ValidatePipelineDefinition",
"datasync:Describe*",
"datasync:List*",
"dax:Describe*",
"dax:ListTags",
"deepracer:ListModels",
"detective:GetGraphIngestState",
"detective:ListGraphs",
"detective:ListMembers",
"devicefarm:ListProjects",
```



```
"directconnect:Describe*",
"discovery:DescribeAgents",
"discovery:DescribeConfigurations",
"discovery:DescribeContinuousExports",
"discovery:DescribeExportConfigurations",
"discovery:DescribeExportTasks",
"discovery:DescribeImportTasks",
"dms:Describe*",
"dms:ListTagsForResource",
"docdb-elastic:ListClusters",
"ds:DescribeDirectories",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeExport",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeKinesisStreamingDestination",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListExports",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetImageBlockPublicAccessState",
"ec2:GetManagedPrefixListAssociations",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ec2:GetTransitGatewayAttachmentPropagations",
"ec2:GetTransitGatewayMulticastDomainAssociations",
"ec2:GetTransitGatewayPrefixListReferences",
"ec2:GetTransitGatewayRouteTableAssociations",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:SearchTransitGatewayRoutes",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeImages",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
```

```
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribeImageScanFindings",
"ecr:DescribeImages",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRegistryPolicy",
"ecr:GetRegistryScanningConfiguration",
"ecr:GetRepositoryPolicy",
"ecr:ListImages",
"ecr:ListTagsForResource",
"ecs:Describe*",
"ecs:List*",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodeGroup",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListNodeGroups",
"eks:ListTagsForResource",
"eks:ListUpdates",
"elastic-inference:DescribeAccelerators",
"elasticache:Describe*",
"elasticache:ListTagsForResource",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:ListTagsForResource",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeAccountPreferences",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticfilesystem:DescribeTags",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:GetAutoTerminationPolicy",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:GetManagedScalingPolicy",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
```

```
"elastictranscoder:ListPipelines",
"emr-serverless:GetApplication",
"emr-serverless:ListApplications",
"emr-serverless:ListJobRuns",
"es:Describe*",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListElasticsearchInstanceTypeDetails",
"es:ListElasticsearchVersions",
"es:ListTags",
"events:Describe*",
"events:List*",
"events:TestEventPattern",
"finspace:ListEnvironments",
"finspace:ListKxEnvironments",
"firehose:Describe*",
"firehose:List*",
"fms:ListComplianceStatus",
"fms:ListPolicies",
"forecast:ListDatasets",
"frauddetector:GetDetectors",
"fsx:Describe*",
"fsx:List*",
"gamelift:ListBuilds",
"gamelift:ListFleets",
"geo:ListMaps",
"glacier:DescribeVault",
"glacier:GetDataRetrievalPolicy",
"glacier:GetVaultAccessPolicy",
"glacier:GetVaultLock",
"glacier:ListVaults",
"globalaccelerator:Describe*",
"globalaccelerator:List*",
"glue:GetCrawlers",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDatabases",
"glue:GetDevEndpoints",
"glue:GetJobs",
"glue:GetResourcePolicy",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTags",
"grafana:ListWorkspaces",
"greengrass:List*",
```

```
"guardduty:DescribePublishingDestination",
"guardduty:Get*",
"guardduty:List*",
"health:DescribeAffectedAccountsForOrganization",
"health:DescribeAffectedEntities",
"health:DescribeAffectedEntitiesForOrganization",
"health:DescribeEntityAggregates",
"health:DescribeEventAggregates",
"health:DescribeEventDetails",
"health:DescribeEventDetailsForOrganization",
"health:DescribeEventTypes",
"health:DescribeEvents",
"health:DescribeEventsForOrganization",
"health:DescribeHealthServiceStatusForOrganization",
"healthlake:ListFHIRDatastores",
"honeycode:ListTables",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"iam:SimulateCustomPolicy",
"iam:SimulatePrincipalPolicy",
"identitystore:ListGroupMemberships",
"identitystore:ListGroupMembershipsForMember",
"identitystore:ListGroups",
"identitystore:ListUsers",
"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",
"inspector:Describe*",
"inspector:Get*",
```

```
"inspector:List*",
"inspector:Preview*",
"iot:Describe*",
"iot:GetPolicy",
"iot:GetPolicyVersion",
"iot:List*",
"iotanalytics:ListChannels",
"iotevents:ListInputs",
"iotfleetwise:ListModelManifests",
"iotsitewise:DescribeGatewayCapabilityConfiguration",
"iotsitewise:ListAssetModels",
"iotsitewise:ListGateways",
"iottwinmaker:ListWorkspaces",
"kafka-cluster:Describe*",
"kafka:Describe*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafkaconnect:Describe*",
"kafkaconnect:List*",
"kendra:DescribeIndex",
"kendra:ListDataSources",
"kendra:ListIndices",
"kendra:ListTagsForResource",
"kinesis:DescribeLimits",
"kinesis:DescribeStream",
"kinesis:DescribeStreamConsumer",
"kinesis:DescribeStreamSummary",
"kinesis:ListShards",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
"kinesisanalytics:ListApplications",
"kinesisanalytics:ListTagsForResource",
"kinesisvideo:DescribeEdgeConfiguration",
"kinesisvideo:DescribeMappedResourceConfiguration",
"kinesisvideo:DescribeMediaStorageConfiguration",
"kinesisvideo:DescribeNotificationConfiguration",
"kinesisvideo:DescribeSignalingChannel",
"kinesisvideo:DescribeStream",
"kinesisvideo:ListSignalingChannels",
"kinesisvideo:ListStreams",
"kinesisvideo:ListTagsForResource",
"kinesisvideo:ListTagsForStream",
```

```
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lambda:GetAccountSettings",
"lambda:GetFunctionConfiguration",
"lambda:GetFunctionEventInvokeConfig",
"lambda:GetLayerVersionPolicy",
"lambda:GetPolicy",
"lambda:List*",
"lex:DescribeBot",
"lex:DescribeResourcePolicy",
"lex:ListBots",
"license-manager:List*",
"lightsail:GetBuckets",
"lightsail:GetContainerServices",
"lightsail:GetDiskSnapshots",
"lightsail:GetDisks",
"lightsail:GetInstances",
"lightsail:GetLoadBalancers",
"logs:Describe*",
"logs:ListTagsForResource",
"logs:ListTagsLogGroup",
"lookoutequipment:ListDatasets",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutvision:ListProjects",
"machinelearning:DescribeMLModels",
"macie2:ListFindings",
"managedblockchain:ListNetworks",
"mechanicalturk:ListHITs",
"mediaconnect:Describe*",
"mediaconnect:List*",
"medialive:ListChannels",
"mediapackage-vod:DescribePackagingGroup",
"mediapackage-vod:ListPackagingGroups",
"mediapackage:DescribeOriginEndpoint",
"mediapackage:ListOriginEndpoints",
"mediastore:GetContainerPolicy",
"mediastore:GetCorsPolicy",
"mediastore:ListContainers",
"memorydb:DescribeClusters",
"mq:DescribeBroker",
"mq:DescribeBrokerEngineTypes",
"mq:DescribeBrokerInstanceOptions",
"mq:DescribeConfiguration",
```

```
"mq:DescribeConfigurationRevision",
"mq:DescribeUser",
"mq:ListBrokers",
"mq:ListConfigurationRevisions",
"mq:ListConfigurations",
"mq:ListTags",
"mq:ListUsers",
"network-firewall:DescribeFirewall",
"network-firewall:DescribeFirewallPolicy",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:DescribeResourcePolicy",
"network-firewall:DescribeRuleGroup",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"network-firewall:ListRuleGroups",
"networkmanager:DescribeGlobalNetworks",
"nimble:ListStudios",
"opsworks-cm:DescribeServers",
"opsworks:DescribeStacks",
"organizations:Describe*",
"organizations:List*",
"personalize:DescribeDatasetGroup",
"personalize:ListDatasetGroups",
"private-networks:ListNetworks",
"profile:GetDomain",
"profile:ListDomains",
"profile:ListIntegrations",
"qlldb:DescribeJournalS3Export",
"qlldb:DescribeLedger",
"qlldb:ListJournalS3Exports",
"qlldb:ListJournalS3ExportsForLedger",
"qlldb:ListLedgers",
"quicksight:Describe*",
"quicksight:List*",
"ram:GetResourceShares",
"ram:List*",
"rds:Describe*",
"rds:DownloadDBLogFilePortion",
"rds:ListTagsForResource",
"redshift-serverless:GetNamespace",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListWorkgroups",
"redshift:Describe*",
"rekognition:Describe*",
```

```
"rekognition:List*",
"resource-groups:ListGroupResources",
"robomaker:Describe*",
"robomaker:List*",
"route53:Get*",
"route53:List*",
"route53domains:GetDomainDetail",
"route53domains:GetOperationDetail",
"route53domains:ListDomains",
"route53domains:ListOperations",
"route53domains:ListTagsForDomain",
"route53resolver:Get*",
"route53resolver:List*",
"s3-outposts:ListEndpoints",
"s3-outposts:ListOutpostsWithS3",
"s3-outposts:ListSharedEndpoints",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetAnalyticsConfiguration",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetInventoryConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMetricsConfiguration",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListMultiRegionAccessPoints",
"sagemaker:Describe*",
"sagemaker:List*",
"schemas:DescribeCodeBinding",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemaVersions",
```



```
"schemas:ListSchemas",
"schemas:ListTagsForResource",
"sdb:DomainMetadata",
"sdb:ListDomains",
"secretsmanager:DescribeSecret",
"secretsmanager:GetResourcePolicy",
"secretsmanager:ListSecretVersionIds",
"secretsmanager:ListSecrets",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"serverlessrepo:GetApplicationPolicy",
"serverlessrepo:List*",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetRequestedServiceQuotaChange",
"servicequotas:GetServiceQuota",
"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"servicequotas:ListTagsForResource",
"ses:Describe*",
"ses:GetAccount",
"ses:GetAccountSendingEnabled",
"ses:GetConfigurationSet",
"ses:GetConfigurationSetEventDestinations",
"ses:GetDedicatedIps",
"ses:GetEmailIdentity",
"ses:GetIdentityDkimAttributes",
"ses:GetIdentityPolicies",
"ses:GetIdentityVerificationAttributes",
"ses:ListConfigurationSets",
"ses:ListDedicatedIpPools",
"ses:ListIdentities",
"ses:ListIdentityPolicies",
"ses:ListReceiptFilters",
"ses:ListReceiptRuleSets",
"ses:ListVerifiedEmailAddresses",
"shield:Describe*",
"shield:GetSubscriptionState",
```

```
"shield:List*",
"snowball:ListClusters",
"snowball:ListJobs",
"sns:GetPlatformApplicationAttributes",
"sns:GetTopicAttributes",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTagsForResource",
"sns:ListTopics",
"sqs:GetQueueAttributes",
"sqs:ListDeadLetterSourceQueues",
"sqs:ListQueueTags",
"sqs:ListQueues",
"ssm:Describe*",
"ssm:GetAutomationExecution",
"ssm:GetServiceSetting",
"ssm:ListAssociationVersions",
"ssm:ListAssociations",
"ssm:ListCommands",
"ssm:ListComplianceItems",
"ssm:ListComplianceSummaries",
"ssm:ListDocumentMetadataHistory",
"ssm:ListDocumentVersions",
"ssm:ListDocuments",
"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:DescribeTrustedAdvisorCheckSummaries",
"support:DescribeTrustedAdvisorChecks",
"synthetics:DescribeCanaries",
"synthetics:DescribeCanariesLastRun",
"synthetics:DescribeRuntimeVersions",
"synthetics:GetCanary",
"synthetics:GetCanaryRuns",
"synthetics:GetGroup",
"synthetics:ListAssociatedGroups",
"synthetics:ListGroupResources",
"synthetics:ListGroups",
"synthetics:ListTagsForResource",
"tag:GetResources",
"tag:GetTagKeys",
"transcribe:GetCallAnalyticsCategory",
"transcribe:GetMedicalVocabulary",
"transcribe:GetVocabulary",
"transcribe:GetVocabularyFilter",
"transcribe:ListCallAnalyticsCategories",
"transcribe:ListCallAnalyticsJobs",
"transcribe:ListLanguageModels",
"transcribe:ListMedicalTranscriptionJobs",
"transcribe:ListMedicalVocabularies",
"transcribe:ListTagsForResource",
"transcribe:ListTranscriptionJobs",
"transcribe:ListVocabularies",
"transcribe:ListVocabularyFilters",
"transfer:Describe*",
"transfer:List*",
"translate:List*",
"trustedadvisor:Describe*",
"voiceid:DescribeDomain",
"waf-regional:GetWebACL",
"waf-regional:ListResourcesForWebACL",
"waf-regional:ListTagsForResource",
```

```

        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAssistant",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
    ],
    "Resource" : "*"
},
{
    "Sid" : "APIGatewayAccess",
    "Effect" : "Allow",
    "Action" : [
        "apigateway:GET"
    ],
    "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
    ]
}

```

```

    "arn:aws:apigateway:*::/apis/*/models/*",
    "arn:aws:apigateway:*::/apis/*/models",
    "arn:aws:apigateway:*::/apis/*/routes/*",
    "arn:aws:apigateway:*::/apis/*/routes",
    "arn:aws:apigateway:*::/apis/*/stages",
    "arn:aws:apigateway:*::/apis/*/stages/*",
    "arn:aws:apigateway:*::/clientcertificates",
    "arn:aws:apigateway:*::/clientcertificates/*",
    "arn:aws:apigateway:*::/domainnames",
    "arn:aws:apigateway:*::/domainnames/*/apimappings",
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/authorizers/*",
    "arn:aws:apigateway:*::/restapis/*/authorizers",
    "arn:aws:apigateway:*::/restapis/*/deployments/*",
    "arn:aws:apigateway:*::/restapis/*/deployments",
    "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
    "arn:aws:apigateway:*::/restapis/*/documentation/parts",
    "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
    "arn:aws:apigateway:*::/restapis/*/documentation/versions",
    "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
    "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
    "arn:aws:apigateway:*::/restapis/*/models/*",
    "arn:aws:apigateway:*::/restapis/*/models",
    "arn:aws:apigateway:*::/restapis/*/requestvalidators",
    "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*",
    "arn:aws:apigateway:*::/restapis/*/resources",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/tags/*",
    "arn:aws:apigateway:*::/vpclinks"
  ]
}
]
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

SecurityLakeServiceLinkedRole

Descrizione: questa politica concede le autorizzazioni per gestire il servizio Amazon Security Lake per tuo conto

SecurityLakeServiceLinkedRole è una politica [AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 29 novembre 2022, 14:03 UTC
- Ora modificata: 19 aprile 2024, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
    },
  ],
}
```

```
"Resource" : [
  "*"
],
{
  "Sid" : "DescribeOrgAccounts",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount"
  ],
  "Resource" : [
    "arn:aws:organizations::*:account/o-*/*"
  ]
},
{
  "Sid" : "AllowManagementOfServiceLinkedChannel",
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:CreateServiceLinkedChannel",
    "cloudtrail>DeleteServiceLinkedChannel",
    "cloudtrail:GetServiceLinkedChannel",
    "cloudtrail:UpdateServiceLinkedChannel"
  ],
  "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
},
{
  "Sid" : "AllowListServiceLinkedChannel",
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:ListServiceLinkedChannels"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DescribeAnyVpc",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ListDelegatedAdmins",
  "Effect" : "Allow",
```

```
"Action" : [
  "organizations:ListDelegatedAdministrators"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
  }
}
},
{
  "Sid" : "AllowWafLoggingConfiguration",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutLoggingConfiguration",
    "wafv2:GetLoggingConfiguration",
    "wafv2:ListLoggingConfigurations",
    "wafv2>DeleteLoggingConfiguration"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "wafv2:LogScope" : "SecurityLake"
    }
  }
},
{
  "Sid" : "AllowPutLoggingConfiguration",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutLoggingConfiguration"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
    }
  }
},
{
  "Sid" : "ListWebACLs",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:ListWebACLs"
  ]
}
```



```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LogDelivery",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs>DeleteLogDelivery"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "wafv2.amazonaws.com"
        ]
      }
    }
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ServerMigration_ServiceRole

Descrizione: Autorizzazioni per consentire al AWS Server Migration Service di migrare le VM verso EC2: consente al Server Migration Service di collocare le risorse migrate nell'account EC2 del cliente.

ServerMigration_ServiceRole [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti ServerMigration_ServiceRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio

- Ora di creazione: 11 agosto 2020, 20:41 UTC
- Ora modificata: 15 ottobre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*/*"
        }
    }
}
]

```

```
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ServerMigrationConnector

Descrizione: Autorizzazioni per consentire al AWS Server Migration Connector di migrare le macchine virtuali su EC2. Consente la comunicazione con il AWS Server Migration Service, l'accesso in lettura/scrittura ai bucket S3 che iniziano con 'sms-b-' e 'import-to-ec2-', nonché ai bucket utilizzati per l'aggiornamento del Server Migration Connector, la registrazione del AWS Server Migration Connector con e il caricamento delle metriche su. AWS AWS AWS

ServerMigrationConnector [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti ServerMigrationConnector ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 ottobre 2016, 21:45 UTC
- Ora modificata: 24 ottobre 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ServerMigrationServiceConsoleFullAccess

Descrizione: autorizzazioni necessarie per utilizzare tutte le funzionalità della Server Migration Service Console

ServerMigrationServiceConsoleFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ServerMigrationServiceConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita

- Ora di creazione: 09 maggio 2020, 17:18 UTC
- Ora modificata: 20 luglio 2020, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ServerMigrationServiceLaunchRole

Descrizione: Autorizzazioni per consentire al Servizio di migrazione dei server AWS di creare e aggiornare AWS le risorse pertinenti presso il cliente Account AWS per l'avvio di server e applicazioni migrati.

ServerMigrationServiceLaunchRole [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti ServerMigrationServiceLaunchRole ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 novembre 2018, 19:53 UTC
- Ora modificata: 15 ottobre 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
    }
  }
}
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ServerMigrationServiceRoleForInstanceValidation

Descrizione: autorizzazioni per consentire all' AWS SMS di eseguire lo script di convalida dei dati utilizzato e di inviare lo script a SMS con esito positivo o negativo

ServerMigrationServiceRoleForInstanceValidation [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti ServerMigrationServiceRoleForInstanceValidation ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 luglio 2020, 22:25 UTC
- Ora modificata: 20 luglio 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ServiceQuotasFullAccess

Descrizione: Fornisce l'accesso completo a Service Quotas

ServiceQuotasFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ServiceQuotasFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2019, 15:44 UTC
- Ora modificata: 04 febbraio 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ServiceQuotasReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Service Quotas

ServiceQuotasReadOnlyAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti ServiceQuotasReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2019, 15:31 UTC
- Ora modificata: 21 dicembre 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ServiceQuotasServiceRolePolicy

Descrizione: consente a Service Quotas di creare casi di assistenza per conto dell'utente

ServiceQuotasServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 22 maggio 2019, 20:44 UTC
- Ora modificata: 24 giugno 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

SimpleWorkflowFullAccess

Descrizione: fornisce l'accesso completo al servizio di configurazione Simple Workflow.

SimpleWorkflowFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti SimpleWorkflowFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

SplitCostAllocationDataServiceRolePolicy

Descrizione: consente ai dati di allocazione dei costi suddivisi di recuperare le informazioni di AWS Organizations, se applicabile, e raccogliere dati di telemetria per i servizi di dati di allocazione dei costi suddivisi per i quali il cliente ha scelto di aderire.

SplitCostAllocationDataServiceRolePolicy [è una politica gestita.AWS](#)

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 16 aprile 2024, 16:05 UTC
- Ora modificata: 16 aprile 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
```



```
{
  "Sid" : "AmazonManagedServiceForPrometheusAccess",
  "Effect" : "Allow",
  "Action" : [
    "aps:ListWorkspaces",
    "aps:QueryMetrics"
  ],
  "Resource" : "*"
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

SupportUser

Descrizione: questo criterio concede le autorizzazioni per la risoluzione dei problemi e la risoluzione di problemi in un. Account AWS Questa politica consente inoltre all'utente di contattare l' AWS assistenza per creare e gestire i casi.

SupportUser è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti SupportUser ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:21 UTC
- Ora modificata: 25 agosto 2023, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

SystemAdministrator

Descrizione: concede le autorizzazioni di accesso complete necessarie per le risorse necessarie per le operazioni di applicazione e sviluppo.

SystemAdministrator è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti SystemAdministrator ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:23 UTC
- Ora modificata: 24 agosto 2020, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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:ReportInstanceState",
"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"
}

```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

TranslateFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Translate.

TranslateFullAccess è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti TranslateFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 23:36 UTC
- Ora modificata: 08 gennaio 2020, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

TranslateReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Translate.

TranslateReadOnly è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti TranslateReadOnly ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 18:22 UTC
- Ora modificata: 24 maggio 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

ViewOnlyAccess

Descrizione: questa politica concede le autorizzazioni per visualizzare risorse e metadati di base in tutti i servizi. AWS

ViewOnlyAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti ViewOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:20 UTC
- Ora modificata: 10 giugno 2024, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Versione della politica

Versione della politica: v19 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
```

```
"backup:DescribeBackupVault",
"backup:DescribeCopyJob",
"backup:DescribeFramework",
"backup:DescribeGlobalSettings",
"backup:DescribeProtectedResource",
"backup:DescribeRecoveryPoint",
"backup:DescribeRegionSettings",
"backup:DescribeReportJob",
"backup:DescribeReportPlan",
"backup:DescribeRestoreJob",
"backup:GetSupportedResourceTypes",
"backup:ListBackupJobs",
"backup:ListBackupPlanTemplates",
"backup:ListBackupPlanVersions",
"backup:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListCopyJobs",
"backup:ListFrameworks",
"backup:ListLegalHolds",
"backup:ListProtectedResources",
"backup:ListProtectedResourcesByBackupVault",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListRecoveryPointsByLegalHold",
"backup:ListRecoveryPointsByResource",
"backup:ListReportJobs",
"backup:ListReportPlans",
"backup:ListRestoreJobs",
"backup:ListTags",
"batch:ListJobs",
"bedrock:ListCustomModels",
"bedrock:ListTagsForResource",
"clouddirectory:ListAppliedSchemaArns",
"clouddirectory:ListDevelopmentSchemaArns",
"clouddirectory:ListDirectories",
"clouddirectory:ListPublishedSchemaArns",
"cloudformation:DescribeStacks",
"cloudformation:List*",
"cloudfront:List*",
"cloudsearch:DescribeDomains",
"cloudsearch:List*",
"cloudtrail:DescribeTrails",
"cloudtrail:ListTrails",
"cloudtrail:LookupEvents",
```

```
"cloudwatch:Get*",
"cloudwatch:List*",
"codebuild:ListBuilds*",
"codebuild:ListProjects",
"codecommit:List*",
"codedeploy:BatchGetApplicationRevisions",
"codedeploy:BatchGetApplications",
"codedeploy:BatchGetDeploymentGroups",
"codedeploy:BatchGetDeploymentInstances",
"codedeploy:BatchGetDeploymentTargets",
"codedeploy:BatchGetDeployments",
"codedeploy:BatchGetOnPremisesInstances",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:ListPipelines",
"codestar:List*",
"cognito-identity:ListIdentities",
"cognito-identity:ListIdentityPools",
"cognito-idp:List*",
"cognito-sync:ListDatasets",
"comprehend:Describe*",
"comprehend:List*",
"config:Describe*",
"config:List*",
"connect:List*",
"cost-optimization-hub:GetPreferences",
"cost-optimization-hub:GetRecommendation",
"cost-optimization-hub:ListEnrollmentStatuses",
"cost-optimization-hub:ListRecommendationSummaries",
"cost-optimization-hub:ListRecommendations",
"databrew:ListJobs",
"databrew:ListProjects",
"datapipeline:DescribePipelines",
"datapipeline:GetAccountLimits",
"datapipeline:ListPipelines",
"dax:DescribeClusters",
"dax:DescribeDefaultParameters",
"dax:DescribeEvents",
"dax:DescribeParameterGroups",
"dax:DescribeParameters",
"dax:DescribeSubnetGroups",
"dax:ListTags",
"devicefarm:List*",
"directconnect:Describe*",
```

```
"discovery:List*",
"dms:List*",
"ds:DescribeDirectories",
"dynamodb:DescribeBackup",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeGlobalTableSettings",
"dynamodb:DescribeLimits",
"dynamodb:DescribeReservedCapacity",
"dynamodb:DescribeReservedCapacityOfferings",
"dynamodb:DescribeStream",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListExports",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeBundleTasks",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeConversionTasks",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeExportTasks",
"ec2:DescribeFlowLogs",
"ec2:DescribeHost*",
"ec2: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:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:ListImages",
"ecs:Describe*",
"ecs:List*",
"eks:ListTagsForResource",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:DescribeAccelerators",
"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*",
"emr-serverless:ListApplications",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
```

```
"es:ListDomainNames",
"events:ListRuleNamesByTarget",
"events:ListRules",
"events:ListTargetsByRule",
"firehose:DescribeDeliveryStream",
"firehose:List*",
"fsx:DescribeFileSystems",
"gamelift:List*",
"glacier:List*",
"glue:GetTags",
"greengrass:List*",
"iam:GetAccountSummary",
"iam:GetLoginProfile",
"iam:List*",
"importexport:ListJobs",
"inspector:List*",
"iot:List*",
"kafka:ListClusters",
"kendra:ListDataSources",
"kendra:ListTagsForResource",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kinesisanalytics:ListTagsForResource",
"kms:ListKeys",
"kms:ListResourceTags",
"lambda:List*",
"lex:GetBotAliases",
"lex:GetBotChannelAssociations",
"lex: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*",
```

```
"logs:ListTagsForResource",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"machinelearning:Describe*",
"mediaconnect:ListEntitlements",
"mediaconnect:ListFlows",
"mediaconnect:ListOfferings",
"mediaconnect:ListReservations",
"mobiletargeting:GetApplicationSettings",
"mobiletargeting:GetCampaigns",
"mobiletargeting:GetImportJobs",
"mobiletargeting:GetSegments",
"oam:ListAttachedLinks",
"oam:ListLinks",
"oam:ListSinks",
"opsworks-cm:Describe*",
"opsworks:Describe*",
"organizations:List*",
"outposts:GetOutpost",
"outposts:GetOutpostInstanceTypes",
"outposts:ListOutposts",
"outposts:ListSites",
"outposts:ListTagsForResource",
"polly:Describe*",
"polly:List*",
"profile:ListDomains",
"profile:ListIntegrations",
"rds:Describe*",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListWorkgroups",
"redshift:DescribeClusters",
"redshift:DescribeEvents",
"redshift:ViewQueriesInConsole",
"resource-explorer-2:GetDefaultView",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListSupportedResourceTypes",
"resource-explorer-2:ListTagsForResource",
"resource-explorer-2:ListViews",
"route53:Get*",
"route53:List*",
"route53domains:List*",
"route53resolver:Get*",
```

```

    "route53resolver:List*",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListMultiRegionAccessPoints",
    "sagemaker:Describe*",
    "sagemaker:List*",
    "sdb:List*",
    "servicecatalog:List*",
    "ses:DescribeActiveReceiptRuleSet",
    "ses:List*",
    "ses:ListDedicatedIpPools",
    "shield:List*",
    "sns:List*",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "sqs:ListDeadLetterSourceQueues",
    "sqs:ListMessageMoveTasks",
    "sqs:ListQueueTags",
    "sqs:ListQueues",
    "ssm:ListAssociations",
    "ssm:ListDocuments",
    "states:ListActivities",
    "states:ListStateMachineAliases",
    "states:ListStateMachineVersions",
    "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*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Sid" : "APIGatewayAccess",

```



```

"Action" : [
  "apigateway:GET"
],
"Resource" : [
  "arn:aws:apigateway:*::/apis",
  "arn:aws:apigateway:*::/apis/*/authorizers/*",
  "arn:aws:apigateway:*::/apis/*/authorizers",
  "arn:aws:apigateway:*::/apis/*/cors",
  "arn:aws:apigateway:*::/apis/*/deployments/*",
  "arn:aws:apigateway:*::/apis/*/deployments",
  "arn:aws:apigateway:*::/apis/*/exports/*",
  "arn:aws:apigateway:*::/apis/*/integrations/*",
  "arn:aws:apigateway:*::/apis/*/integrations",
  "arn:aws:apigateway:*::/apis/*/models/*",
  "arn:aws:apigateway:*::/apis/*/models",
  "arn:aws:apigateway:*::/apis/*/routes/*",
  "arn:aws:apigateway:*::/apis/*/routes",
  "arn:aws:apigateway:*::/apis/*/stages",
  "arn:aws:apigateway:*::/apis/*/stages/*",
  "arn:aws:apigateway:*::/clientcertificates",
  "arn:aws:apigateway:*::/clientcertificates/*",
  "arn:aws:apigateway:*::/domainnames",
  "arn:aws:apigateway:*::/domainnames/*/apimappings",
  "arn:aws:apigateway:*::/restapis",
  "arn:aws:apigateway:*::/restapis/*/authorizers/*",
  "arn:aws:apigateway:*::/restapis/*/authorizers",
  "arn:aws:apigateway:*::/restapis/*/deployments/*",
  "arn:aws:apigateway:*::/restapis/*/deployments",
  "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
  "arn:aws:apigateway:*::/restapis/*/documentation/parts",
  "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
  "arn:aws:apigateway:*::/restapis/*/documentation/versions",
  "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
  "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
  "arn:aws:apigateway:*::/restapis/*/models/*",
  "arn:aws:apigateway:*::/restapis/*/models",
  "arn:aws:apigateway:*::/restapis/*/requestvalidators",
  "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
  "arn:aws:apigateway:*::/restapis/*/resources/*",
  "arn:aws:apigateway:*::/restapis/*/resources",
  "arn:aws:apigateway:*::/restapis/*/stages",
  "arn:aws:apigateway:*::/restapis/*/stages/*",
  "arn:aws:apigateway:*::/tags/*",
  "arn:aws:apigateway:*::/vpclinks"
]

```

```
]
  }
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

VMImportExportRoleForAWSConnector

Descrizione: policy predefinita per il ruolo del servizio VM Import/Export, per i clienti che utilizzano il Connector. AWS Il servizio VM Import/Export assume un ruolo con questa policy per soddisfare le richieste di migrazione delle macchine virtuali dall'appliance virtuale Connector. AWS (Si noti che il AWS Connector utilizza la policy gestita AWSConnector "" per inviare richieste per conto del cliente al servizio VM Import/Export.) Offre la possibilità di creare AMI e snapshot EBS, modificare gli attributi degli snapshot EBS, effettuare chiamate «Describe*» su oggetti EC2 e leggere dai bucket S3 che iniziano con '2-'. import-to-ec

VMImportExportRoleForAWSConnector [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti VMImportExportRoleForAWSConnector ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica del ruolo di servizio
- Ora di creazione: 3 settembre 2015, 20:48 UTC
- Ora modificata: 3 settembre 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

VPCLatticeFullAccess

Descrizione: fornisce l'accesso completo ad Amazon VPC Lattice e l'accesso ai servizi di dipendenza.

VPCLatticeFullAccess [è una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti VPCLatticeFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 marzo 2023, 02:49 UTC
- Ora modificata: 30 marzo 2023, 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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"
  }
]
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

VPCLatticeReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon VPC Lattice tramite i servizi di dipendenza e accesso limitato ai AWS Management Console servizi di dipendenza.

VPCLatticeReadOnlyAccess [è una politica gestita.AWS](#)

Utilizzo di questa politica

Puoi collegarti VPCLatticeReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 marzo 2023, 02:47 UTC
- Ora modificata: 30 marzo 2023, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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" : "*"
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

VPCLatticeServicesInvokeAccess

Descrizione: fornisce l'accesso per richiamare i servizi Amazon VPC Lattice.

VPCLatticeServicesInvokeAccess è [una politica gestita AWS](#).

Utilizzo di questa politica

Puoi collegarti VPCLatticeServicesInvokeAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 30 marzo 2023, 02:45 UTC
- Ora modificata: 30 marzo 2023, 02:45 UTC

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

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

WAFLoggingServiceRolePolicy

Descrizione: creazione di una SLR per scrivere i log dei clienti in un flusso Firehose

WAFLoggingServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 agosto 2018, 21:05 UTC
- Ora modificata: 24 agosto 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

WAFRegionalLoggingServiceRolePolicy

Descrizione: creazione di una SLR per scrivere i log dei clienti in un flusso Firehose

WAFRegionalLoggingServiceRolePolicy [è una politica gestita AWS](#).

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 24 agosto 2018, 18:40 UTC
- Ora modificata: 24 agosto 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord",
      "firehose:PutRecordBatch"
    ],
    "Resource" : [
      "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
    ]
  }
]
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

WAFV2LoggingServiceRolePolicy

Descrizione: questa policy crea un ruolo collegato al servizio che consente a AWS WAF di scrivere log su Amazon Kinesis Data Firehose.

WAFV2LoggingServiceRolePolicy [AWS è una politica](#) gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della politica

- Tipo: politica relativa ai ruoli collegati ai servizi
- Ora di creazione: 07 novembre 2019, 00:40 UTC
- Ora modificata: 03 giugno 2024, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FirehoseAPIStatement",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "DescribeOrganizationAPIStatement",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

WellArchitectedConsoleFullAccess

Descrizione: Fornisce accesso completo a AWS Well-Architected Tool tramite AWS Management Console

WellArchitectedConsoleFullAccess è una politica [AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti WellArchitectedConsoleFullAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2018, 18:19 UTC
- Ora modificata: 29 novembre 2018, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

```
]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

WellArchitectedConsoleReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura a Well-Architected AWS Tool tramite AWS Management Console

WellArchitectedConsoleReadOnlyAccess [è una politica gestita AWS](#)

Utilizzo di questa politica

Puoi collegarti WellArchitectedConsoleReadOnlyAccess ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2018, 18:21 UTC
- Ora modificata: 29 giugno 2023, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

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

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)
- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

WorkLinkServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon WorkLink

WorkLinkServiceRolePolicy è una [politica AWS gestita](#).

Utilizzo di questa politica

Puoi collegarti WorkLinkServiceRolePolicy ai tuoi utenti, gruppi e ruoli.

Dettagli della politica

- Tipo: politica AWS gestita
- Ora di creazione: 23 gennaio 2019, 19:03 UTC

- Ora modificata: 23 gennaio 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy 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-*"
    }
  ]
}
```

Ulteriori informazioni

- [Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center](#)

- [Aggiungere e rimuovere i permessi di identità IAM](#)
- [Comprendi il controllo delle versioni per le politiche IAM](#)
- [Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi](#)

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.