aws

參考指南

AWS 受管理策略

AWS 受管理策略: 參考指南

Table of Contents

什麼是AWS受管政策？

受AWS管理的策略是由建立和管理的獨立策略AWS。 AWS受管理的政策旨在為許多常見使用案例提供權限。與您必須自行撰寫原則相比，它們可讓您更輕鬆地開始將權限指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予您特定使用案例的最低權限許可，因為它們可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法更改 AWS 受管政策中定義的許可。如果 AWS 更新了 AWS 受管政策中定義的許可，則該更新會影響政策附加的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

瞭解政策參照頁面

每個策略參考頁面都包含下列資訊：

- 使用此策略 — 您是否可以將策略附加到使用者、群組和角色
- 政策詳情
  - 類型 — 受AWS管理策略的類型
    - `AWS managed policy`— 標準的AWS管理策略
    - `Job function policy`— 符合常見行業工作職能的政策
    - `Service-linked role policy`— 附加至服務連結角色的原則，可讓服務代表您執行動作，例如 the section called “AmazonRDSPreviewServiceRolePolicy”
    - `Service role policy`— 旨在與服務角色一起使用的策略，例如 the section called “AWSControlTowerServiceRolePolicy”
  - 建立時間 — 第一次建立原則的時間
  - 編輯時間 — 編輯此版本的策略時間
  - ARN — 政策的 Amazon 資源名稱
- 策略版本 — 策略授與的權限版本
- JSON 政策文件 — 政策 JSON
- 深入瞭解 — 與AWS受管政策相關的文件連結

已廢除的 AWS 受管政策

AWS定期更新AWS受管理的策略。在大多數情況下，我們會將權限新增至政策。當我們啟動新服務或功能時，就會發生這種情況。為了改善受AWS管原則的安全性，我們有時會縮減原則的範圍。當我們從原則中移除權限時，我們會將原則設定為已取代狀態，並提供新的狀態。AWS淘汰某項服務或功能時，我們也會取代該功能的AWS受管政策。

如果您收到電子郵件通知，指出您正在使用的策略已被取代，我們建議您立即採取行動。識別政策的變更並更新您的工作流程。如果AWS提供取代原則，請規劃將其附加至所有受影響的身分識別 (使用者、群組和角色)，然後將已停用的原則與這些身分中斷連結。

已作廢的政策具有以下特點：

- 它已從本指南中移除。
- 權限會繼續適用於所有目前連結的身分識別。
- 在將政策附加至身分的帳戶中，該政策會顯示在 IAM 主控台的「政策」清單中，旁邊會顯示警告圖示。
- 它不能附加到任何新的身份。如果將其與目前的識別分離，則無法將其重新貼附。
- 將其與所有目前圖元分離後，將不再可見。

AWS 受管理政策

AWS 受管理政策

- 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
- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess

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

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

- AmazonEventBridgePipesOperatorAccess
- AmazonEventBridgePipesReadOnlyAccess
- AmazonEventBridgeReadOnlyAccess
- AmazonEventBridgeSchedulerFullAccess
- AmazonEventBridgeSchedulerReadOnlyAccess
- AmazonEventBridgeSchemasFullAccess
- AmazonEventBridgeSchemasReadOnlyAccess
- AmazonEventBridgeSchemasServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess
- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess
- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess
- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess
- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyMalwareProtectionServiceRolePolicy
- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess

- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess
- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ReadOnlyAccess
- AmazonInspector2ServiceRolePolicy
- AmazonInspectorFullAccess
- AmazonInspectorReadOnlyAccess
- AmazonInspectorServiceRolePolicy
- AmazonKendraFullAccess
- AmazonKendraReadOnlyAccess
- AmazonKeyspacesFullAccess
- AmazonKeyspacesReadOnlyAccess
- AmazonKeyspacesReadOnlyAccess_v2
- AmazonKinesisAnalyticsFullAccess
- AmazonKinesisAnalyticsReadOnly
- AmazonKinesisFirehoseFullAccess
- AmazonKinesisFirehoseReadOnlyAccess
- AmazonKinesisFullAccess
- AmazonKinesisReadOnlyAccess
- AmazonKinesisVideoStreamsFullAccess
- AmazonKinesisVideoStreamsReadOnlyAccess
- AmazonLaunchWizard_Fullaccess
- AmazonLaunchWizardFullAccessV2

- AmazonLexChannelsAccess
- AmazonLexFullAccess
- AmazonLexReadOnly
- AmazonLexReplicationPolicy
- AmazonLexRunBotsOnly
- AmazonLexV2BotPolicy
- AmazonLookoutEquipmentFullAccess
- AmazonLookoutEquipmentReadOnlyAccess
- AmazonLookoutMetricsFullAccess
- AmazonLookoutMetricsReadOnlyAccess
- AmazonLookoutVisionConsoleFullAccess
- AmazonLookoutVisionConsoleReadOnlyAccess
- AmazonLookoutVisionFullAccess
- AmazonLookoutVisionReadOnlyAccess
- AmazonMachineLearningBatchPredictionsAccess
- AmazonMachineLearningCreateOnlyAccess
- AmazonMachineLearningFullAccess
- AmazonMachineLearningManageRealTimeEndpointOnlyAccess
- AmazonMachineLearningReadOnlyAccess
- AmazonMachineLearningRealTimePredictionOnlyAccess
- AmazonMachineLearningRoleforRedshiftDataSourceV3
- AmazonMacieFullAccess
- AmazonMacieHandshakeRole
- AmazonMacieReadOnlyAccess
- AmazonMacieServiceRole
- AmazonMacieServiceRolePolicy
- AmazonManagedBlockchainConsoleFullAccess
- AmazonManagedBlockchainFullAccess
- AmazonManagedBlockchainReadOnlyAccess
- AmazonManagedBlockchainServiceRolePolicy

- AmazonMCSFullAccess
- AmazonMCSReadOnlyAccess
- AmazonMechanicalTurkFullAccess
- AmazonMechanicalTurkReadOnly
- AmazonMemoryDBFullAccess
- AmazonMemoryDBReadOnlyAccess
- AmazonMobileAnalyticsFinancialReportAccess
- AmazonMobileAnalyticsFullAccess
- AmazonMobileAnalyticsNon-financialReportAccess
- AmazonMobileAnalyticsWriteOnlyAccess
- AmazonMonitronFullAccess
- AmazonMQApiFullAccess
- AmazonMQApiReadOnlyAccess
- AmazonMQFullAccess
- AmazonMQReadOnlyAccess
- AmazonMQServiceRolePolicy
- AmazonMSKConnectReadOnlyAccess
- AmazonMSKFullAccess
- AmazonMSKReadOnlyAccess
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess
- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- 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
- AmazonRDSDataFullAccess
- AmazonRDSDirectoryServiceAccess
- AmazonRDSEnhancedMonitoringRole
- AmazonRDSFullAccess
- AmazonRDSPerformanceInsightsFullAccess
- AmazonRDSPerformanceInsightsReadOnly

- AmazonRDSPreviewServiceRolePolicy
- AmazonRDSReadOnlyAccess
- AmazonRDSServiceRolePolicy
- AmazonRedshiftAllCommandsFullAccess
- AmazonRedshiftDataFullAccess
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing
- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess
- AmazonRoute53FullAccess
- AmazonRoute53ProfilesFullAccess
- AmazonRoute53ProfilesReadOnlyAccess
- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess
- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess

- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess
- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy
- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess
- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole
- AmazonSageMakerGeospatialFullAccess
- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSecurityLakeAdministrator
- AmazonSecurityLakeMetastoreManager
- AmazonSecurityLakePermissionsBoundary
- AmazonSESFullAccess
- AmazonSESReadOnlyAccess
- AmazonSNSFullAccess
- AmazonSNSReadOnlyAccess
- AmazonSNSRole
- AmazonSQSFullAccess
- AmazonSQSReadOnlyAccess
- AmazonSSMAutomationApproverAccess
- AmazonSSMAutomationRole
- AmazonSSMDirectoryServiceAccess
- AmazonSSMFullAccess
- AmazonSSMMaintenanceWindowRole
- AmazonSSMManagedEC2InstanceDefaultPolicy
- AmazonSSMManagedInstanceCore
- AmazonSSMPatchAssociation
- AmazonSSMReadOnlyAccess

- AmazonSSMServiceRolePolicy
- AmazonSumerianFullAccess
- AmazonTextractFullAccess
- AmazonTextractServiceRole
- AmazonTimestreamConsoleFullAccess
- AmazonTimestreamFullAccess
- AmazonTimestreamInfluxDBFullAccess
- AmazonTimestreamInfluxDBServiceRolePolicy
- AmazonTimestreamReadOnlyAccess
- AmazonTranscribeFullAccess
- AmazonTranscribeReadOnlyAccess
- AmazonVPCCrossAccountNetworkInterfaceOperations
- AmazonVPCFullAccess
- AmazonVPCNetworkAccessAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
- AmazonVPCReadOnlyAccess
- AmazonWorkDocsFullAccess
- AmazonWorkDocsReadOnlyAccess
- AmazonWorkMailEventsServiceRolePolicy
- AmazonWorkMailFullAccess
- AmazonWorkMailMessageFlowFullAccess
- AmazonWorkMailMessageFlowReadOnlyAccess
- AmazonWorkMailReadOnlyAccess
- AmazonWorkSpacesAdmin
- AmazonWorkSpacesApplicationManagerAdminAccess
- AmazonWorkspacesPCAAccess
- AmazonWorkSpacesSelfServiceAccess
- AmazonWorkSpacesServiceAccess
- AmazonWorkSpacesWebReadOnly

- AmazonWorkSpacesWebServiceRolePolicy
- AmazonZocaloFullAccess
- AmazonZocaloReadOnlyAccess
- AmplifyBackendDeployFullAccess
- APIGatewayServiceRolePolicy
- AppIntegrationsServiceLinkedRolePolicy
- ApplicationAutoScalingForAmazonAppStreamAccess
- ApplicationDiscoveryServiceContinuousExportServiceRolePolicy
- AppRunnerNetworkingServiceRolePolicy
- AppRunnerServiceRolePolicy
- AutoScalingConsoleFullAccess
- AutoScalingConsoleReadOnlyAccess
- AutoScalingFullAccess
- AutoScalingNotificationAccessRole
- AutoScalingReadOnlyAccess
- AutoScalingServiceRolePolicy
- AWS_ConfigRole
- AWSAccountActivityAccess
- AWSAccountManagementFullAccess
- AWSAccountManagementReadOnlyAccess
- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- AWSAppFabricFullAccess
- AWSAppFabricReadOnlyAccess
- AWSAppFabricServiceRolePolicy
- AWSApplicationAutoscalingAppStreamFleetPolicy
- AWSApplicationAutoscalingCassandraTablePolicy
- AWSApplicationAutoscalingComprehendEndpointPolicy
- AWSApplicationAutoScalingCustomResourcePolicy
- AWSApplicationAutoscalingDynamoDBTablePolicy

- AWSApplicationAutoscalingEC2SpotFleetRequestPolicy
- AWSApplicationAutoscalingECSServicePolicy
- AWSApplicationAutoscalingElastiCacheRGPolicy
- AWSApplicationAutoscalingEMRInstanceGroupPolicy
- AWSApplicationAutoscalingKafkaClusterPolicy
- AWSApplicationAutoscalingLambdaConcurrencyPolicy
- AWSApplicationAutoscalingNeptuneClusterPolicy
- AWSApplicationAutoscalingRDSClusterPolicy
- AWSApplicationAutoscalingSageMakerEndpointPolicy
- AWSApplicationDiscoveryAgentAccess
- AWSApplicationDiscoveryAgentlessCollectorAccess
- AWSApplicationDiscoveryServiceFullAccess
- AWSApplicationMigrationAgentInstallationPolicy
- AWSApplicationMigrationAgentPolicy
- AWSApplicationMigrationAgentPolicy_v2
- AWSApplicationMigrationConversionServerPolicy
- AWSApplicationMigrationEC2Access
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess
- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy
- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy
- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess
- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly

- AWSAppMeshServiceRolePolicy
- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess
- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole

- AWSBatchServiceRole
- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingReadOnlyAccess
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBugBustFullAccess
- AWSBugBustPlayerAccess
- AWSBugBustServiceRolePolicy
- AWSCertificateManagerFullAccess
- AWSCertificateManagerPrivateCAAuditor
- AWSCertificateManagerPrivateCAFullAccess
- AWSCertificateManagerPrivateCAPrivilegedUser
- AWSCertificateManagerPrivateCAReadOnly
- AWSCertificateManagerPrivateCAUser
- AWSCertificateManagerReadOnly
- AWSChatbotServiceLinkedRolePolicy
- AWSCleanRoomsFullAccess
- AWSCleanRoomsFullAccessNoQuerying
- AWSCleanRoomsMLFullAccess
- AWSCleanRoomsMLReadOnlyAccess
- AWSCleanRoomsReadOnlyAccess
- AWSCloud9Administrator
- AWSCloud9EnvironmentMember
- AWSCloud9ServiceRolePolicy
- AWSCloud9SSMInstanceProfile
- AWSCloud9User
- AWSCloudFormationFullAccess
- AWSCloudFormationReadOnlyAccess

- AWSCloudFrontLogger
- AWSCloudHSMFullAccess
- AWSCloudHSMReadOnlyAccess
- AWSCloudHSMRole
- AWSCloudMapDiscoverInstanceAccess
- AWSCloudMapFullAccess
- AWSCloudMapReadOnlyAccess
- AWSCloudMapRegisterInstanceAccess
- AWSCloudShellFullAccess
- AWSCloudTrail_FullAccess
- AWSCloudTrail_ReadOnlyAccess
- AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy
- AWSCodeArtifactAdminAccess
- AWSCodeArtifactReadOnlyAccess
- AWSCodeBuildAdminAccess
- AWSCodeBuildDeveloperAccess
- AWSCodeBuildReadOnlyAccess
- AWSCodeCommitFullAccess
- AWSCodeCommitPowerUser
- AWSCodeCommitReadOnly
- AWSCodeDeployDeployerAccess
- AWSCodeDeployFullAccess
- AWSCodeDeployReadOnlyAccess
- AWSCodeDeployRole
- AWSCodeDeployRoleForCloudFormation
- AWSCodeDeployRoleForECS
- AWSCodeDeployRoleForECSLimited
- AWSCodeDeployRoleForLambda
- AWSCodeDeployRoleForLambdaLimited
- AWSCodePipeline_FullAccess

- AWSCodePipeline_ReadOnlyAccess
- AWSCodePipelineApproverAccess
- AWSCodePipelineCustomActionAccess
- AWSCodeStarFullAccess
- AWSCodeStarNotificationsServiceRolePolicy
- AWSCodeStarServiceRole
- AWSCompromisedKeyQuarantine
- AWSCompromisedKeyQuarantineV2
- AWSConfigMultiAccountSetupPolicy
- AWSConfigRemediationServiceRolePolicy
- AWSConfigRoleForOrganizations
- AWSConfigRulesExecutionRole
- AWSConfigServiceRolePolicy
- AWSConfigUserAccess
- AWSConnector
- AWSControlTowerAccountServiceRolePolicy
- AWSControlTowerServiceRolePolicy
- AWSCostAndUsageReportAutomationPolicy
- AWSDataExchangeFullAccess
- AWSDataExchangeProviderFullAccess
- AWSDataExchangeReadOnly
- AWSDataExchangeSubscriberFullAccess
- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccess
- AWSDataPipeline_FullAccess
- AWSDataPipeline_PowerUser
- AWSDataSyncDiscoveryServiceRolePolicy
- AWSDataSyncFullAccess
- AWSDataSyncReadOnlyAccess

- 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
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy

- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy
- AWSElasticDisasterRecoveryReplicationServerPolicy
- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConvertFullAccess
- AWSElementalMediaConvertReadOnly
- AWSElementalMediaLiveFullAccess
- AWSElementalMediaLiveReadOnly
- AWSElementalMediaPackageFullAccess
- AWSElementalMediaPackageReadOnly
- AWSElementalMediaPackageV2FullAccess
- AWSElementalMediaPackageV2ReadOnly
- AWSElementalMediaStoreFullAccess
- AWSElementalMediaStoreReadOnly
- AWSElementalMediaTailorFullAccess
- AWSElementalMediaTailorReadOnly
- AWSEnhancedClassicNetworkingMangementPolicy
- AWSEntityResolutionConsoleFullAccess
- AWSEntityResolutionConsoleReadOnlyAccess
- AWSFaultInjectionSimulatorEC2Access
- AWSFaultInjectionSimulatorECSAccess
- AWSFaultInjectionSimulatorEKSAccess
- AWSFaultInjectionSimulatorNetworkAccess
- AWSFaultInjectionSimulatorRDSAccess
- AWSFaultInjectionSimulatorSSMAccess
- AWSFinSpaceServiceRolePolicy

- AWSFMAdminFullAccess
- AWSFMAdminReadOnlyAccess
- AWSFMMemberReadOnlyAccess
- AWSForWordPressPluginPolicy
- AWSGitSyncServiceRolePolicy
- AWSGlobalAcceleratorSLRPolicy
- AWSGlueConsoleFullAccess
- AWSGlueConsoleSageMakerNotebookFullAccess
- AwsGlueDataBrewFullAccessPolicy
- AWSGlueDataBrewServiceRole
- AWSGlueSchemaRegistryFullAccess
- AWSGlueSchemaRegistryReadonlyAccess
- AWSGlueServiceNotebookRole
- AWSGlueServiceRole
- AwsGlueSessionUserRestrictedNotebookPolicy
- AwsGlueSessionUserRestrictedNotebookServiceRole
- AwsGlueSessionUserRestrictedPolicy
- AwsGlueSessionUserRestrictedServiceRole
- AWSGrafanaAccountAdministrator
- AWSGrafanaConsoleReadOnlyAccess
- AWSGrafanaWorkspacePermissionManagement
- AWSGrafanaWorkspacePermissionManagementV2
- AWSGreengrassFullAccess
- AWSGreengrassReadOnlyAccess
- AWSGreengrassResourceAccessRolePolicy
- AWSGroundStationAgentInstancePolicy
- AWSHealth_EventProcessorServiceRolePolicy
- AWSHealthFullAccess
- AWSHealthImagingFullAccess
- AWSHealthImagingReadOnlyAccess

- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIdentitySyncFullAccess
- AWSIdentitySyncReadOnlyAccess
- AWSImageBuilderFullAccess
- AWSImageBuilderReadOnlyAccess
- AWSImportExportFullAccess
- AWSImportExportReadOnlyAccess
- AWSIncidentManagerIncidentAccessServiceRolePolicy
- AWSIncidentManagerResolverAccess
- AWSIncidentManagerServiceRolePolicy
- AWSIoT1ClickFullAccess
- AWSIoT1ClickReadOnlyAccess
- AWSIoTAnalyticsFullAccess
- AWSIoTAnalyticsReadOnlyAccess
- AWSIoTConfigAccess
- AWSIoTConfigReadOnlyAccess
- AWSIoTDataAccess
- AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction
- AWSIoTDeviceDefenderAudit
- AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction
- AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
- AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction
- AWSIoTDeviceDefenderUpdateCACertMitigationAction
- AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction
- AWSIoTDeviceTesterForFreeRTOSFullAccess
- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy

- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly
- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions
- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess
- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager
- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess
- AWSIPAMServiceRolePolicy
- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy
- AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy
- AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy
- AWSKeyManagementServicePowerUser
- AWSLakeFormationCrossAccountManager
- AWSLakeFormationDataAdmin
- AWSLambda_FullAccess

- AWSLambda_ReadOnlyAccess
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaKinesisExecutionRole
- AWSLambdaMSKExecutionRole
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy
- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy

- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- AWSMediaConnectServicePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess
- AWSMigrationHubFullAccess
- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector
- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess
- AWSMobileHub_ReadOnly
- AWSMSKReplicatorExecutionRole

- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess
- AWSNetworkManagerServiceRolePolicy
- AWSOpsWorks_FullAccess
- AWSOpsWorksCloudWatchLogs
- AWSOpsWorksCMInstanceProfileRole
- AWSOpsWorksCMServiceRole
- AWSOpsWorksInstanceRegistration
- AWSOpsWorksRegisterCLI_EC2
- AWSOpsWorksRegisterCLI_OnPremises
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser

- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess

- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAmazonEKSNodegroup
- 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
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess
- AWSStepFunctionsReadOnlyAccess
- AWSStorageGatewayFullAccess

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

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

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

- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly
- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- 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
- PartnerCentralAccountManagementUserRoleAssociation
- PowerUserAccess
- QBusinessServiceRolePolicy
- QuickSightAccessForS3StorageManagementAnalyticsReadOnly
- RDSCloudHsmAuthorizationRole
- ReadOnlyAccess
- ResourceGroupsandTagEditorFullAccess
- ResourceGroupsandTagEditorReadOnlyAccess
- ResourceGroupsServiceRolePolicy
- ROSAAmazonEBSCSIDriverOperatorPolicy

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

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

AccessAnalyzerServiceRolePolicy

說明：允許存取分析器分析資源中繼資料

`AccessAnalyzerServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十二月二日, 17:13 世界標準時
- 編輯時間：世界標準時間 2024 年 1 月 22 日 22:34
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

政策版本

策略版本：v12(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AdministratorAccess

描述：提供對 AWS 服務和資源的完整存取權。

AdministratorAccess是AWS 受管理的策略。

使用此政策

您可以附加AdministratorAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間:2015 年 2 月 6 日, 18:39 世界標準時間
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AdministratorAccess-Amplify

說明：授予帳戶管理權限，同時明確允許直接存取 Amplify 應用程式所需的資源。

`AdministratorAccess-Amplify`是AWS 受管理的策略。

使用此政策

您可以附加`AdministratorAccess-Amplify`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月 1 日, 世界標準時間 19:03
- 編輯時間：2024 年 4 月 4 日，世界標準時間 20:35
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

政策版本

策略版本：v12(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AdministratorAccess-AWSElasticBeanstalk

描述：授與帳戶管理權限。明確允許開發人員和管理員直接存取管理 E AWS lastic Beanstalk 應用程式所需的資源

AdministratorAccess-AWSElasticBeanstalk是AWS 受管理的策略。

使用此政策

您可以附加AdministratorAccess-AWSElasticBeanstalk至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 1 月 22 日, 世界標準時間 19:36
- 編輯時間：世界標準時間 2023 年 3 月 23 日 23:45
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AlexaForBusinessDeviceSetup

描述：提供 AlexaForBusiness 服務的裝置設定存取權

AlexaForBusinessDeviceSetup是AWS 受管理的策略。

使用此政策

您可以附加AlexaForBusinessDeviceSetup至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月三十日，世界標準時間 16:47
- 編輯時間：2019 年 5 月 20 日，世界標準時間 21:05
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AlexaForBusinessFullAccess

描述：授予對 AlexaForBusiness 資源的完整存取權限和相關存取權 AWS 服務

`AlexaForBusinessFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AlexaForBusinessFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月三十日，世界標準時間 16:47
- 編輯時間:2020 年 7 月 1 日, 世界標準時間 21:01
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AlexaForBusinessGatewayExecution

說明：提供 AlexaForBusiness 服務的閘道執行存取權

`AlexaForBusinessGatewayExecution`是AWS 受管理的策略。

使用此政策

您可以附加`AlexaForBusinessGatewayExecution`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月三十日，世界標準時間 16:47
- 編輯時間：2017 年十一月三十日，世界標準時間 16:47
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AlexaForBusinessLifesizeDelegatedAccessPolicy

說明：提供對生命化 AVS 設備的訪問

`AlexaForBusinessLifesizeDelegatedAccessPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AlexaForBusinessLifesizeDelegatedAccessPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 4 日, 世界標準時間 19:46
- 編輯時間：2020 年 6 月 12 日，世界標準時間 20:31
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IWO7UEGWV4TL"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "a4b:filters_deviceType" : [
            "*A2IWO7UEGWV4TL"
          ]
        },
        "Null" : {
          "a4b:filters_deviceType" : "false"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:GetRoom",
        "a4b:GetAddressBook",
        "a4b:SearchRooms",
        "a4b:CreateContact",
        "a4b:CreateRoom",
        "a4b:UpdateContact",
        "a4b:ListConferenceProviders",
        "a4b:DeleteRoom",
        "a4b:CreateAddressBook",
        "a4b:DisassociateContactFromAddressBook",
        "a4b:CreateConferenceProvider",
        "a4b:PutConferencePreference",
        "a4b:DeleteAddressBook",
        "a4b:AssociateContactWithAddressBook",
        "a4b:DeleteContact",
        "a4b:SearchProfiles",
        "a4b:UpdateProfile",
        "a4b:GetContact"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AlexaForBusinessNetworkProfileServicePolicy

描述：此原則可讓 Alexa for Business 版執行網路設定檔排程的自動化工作。

`AlexaForBusinessNetworkProfileServicePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2019 年 3 月 13 日，世界標準時間 00:53
- 編輯時間：2019 年 4 月 5 日，世界標準時間 21:57
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AlexaForBusinessPolyDelegatedAccessPolicy

說明：提供對聚 AVS 設備的訪問

AlexaForBusinessPolyDelegatedAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AlexaForBusinessPolyDelegatedAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十月十六日, 19:48 世界標準時
- 編輯時間：2019 年 10 月 16 日，世界標準時間 19:48
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AlexaForBusinessReadOnlyAccess

說明：提供 AlexaForBusiness 服務的唯讀存取權

`AlexaForBusinessReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AlexaForBusinessReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月三十日，世界標準時間 16:47
- 編輯時間：2019 年十一月二十日，世界標準時間 00:25
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAPIGatewayAdministrator

說明：提供在 Amazon API 閘道中建立/編輯/刪除 API 的完整存取權，可透過. AWS Management Console

AmazonAPIGatewayAdministrator是AWS 受管理的策略。

使用此政策

您可以附加AmazonAPIGatewayAdministrator至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 7 月 9 日, 17:34 世界標準時間
- 編輯時間:2015 年 7 月 9 日, 17:34 世界標準時間
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAPIGatewayInvokeFullAccess

說明：提供在 Amazon API 閘道中叫用 API 的完整存取權。

AmazonAPIGatewayInvokeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAPIGatewayInvokeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 7 月 9 日, 17:36 世界標準時間
- 編輯時間:2018 年十二月十八日, 世界標準時間 18:25
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAPIGatewayPushToCloudWatchLogs

說明：允許 API Gateway 將記錄推送到使用者的帳戶。

AmazonAPIGatewayPushToCloudWatchLogs是AWS 受管理的策略。

使用此政策

您可以附加AmazonAPIGatewayPushToCloudWatchLogs至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 11 月 11 日, 世界標準時間 23:41
- 編輯時間：2015 年 11 月 11 日，世界標準時間 23:41
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAppFlowFullAccess

說明：提供對 Amazon 的完整存取權，以 AppFlow 及存取作為流程來源或目標 (S3 和 Redshift) 支援的 AWS 服務。還提供對 KMS 進行加密的訪問

AmazonAppFlowFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAppFlowFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 2 日, 世界標準時間 23:30
- 編輯時間：世界標準時間 2022 年 2 月 28 日 23:11
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAppFlowReadOnlyAccess

說明：提供對 Amazon 應用程序流程的唯讀訪問權限

AmazonAppFlowReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAppFlowReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 2 日, 世界標準時間 23:26
- 編輯時間：2022 年 2 月 28 日，世界標準時間 20:42
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAppStreamFullAccess

描述：提供完全訪問 Amazon AppStream 通過 AWS Management Console.

AmazonAppStreamFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAppStreamFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間:2020 年 8 月 28 日, 世界標準時間 17:24
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamFullAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAppStreamPCAAccess

說明：Amazon AppStream 2.0 存取客戶帳戶中的 Certificate Manager 私有 CA，以進行 AWS 憑證型身份驗證

AmazonAppStreamPCAAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAppStreamPCAAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：2022 年 10 月 24 日，下午 17 點
- 編輯時間：2022 年十月二十四日，世界標準時間 17：05
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAppStreamReadOnlyAccess

說明：提供 AppStream 透過 Amazon 的唯讀存取權限 AWS Management Console。

AmazonAppStreamReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAppStreamReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間:二零一六年十二月七日, 21:00 世界標準
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAppStreamServiceAccess

描述：Amazon AppStream 服務角色的預設政策。

AmazonAppStreamServiceAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAppStreamServiceAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略

- **創建時間**:二零一六年十一月十九日, 04:17 世界標準
- **編輯時間**：2020 年 6 月 26 日，世界標準時間 16:33
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAthenaFullAccess

描述：提供對 Amazon Athena 的完整存取權限，以及啟用查詢、寫入結果和資料管理所需的相依性範圍存取權限。

AmazonAthenaFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAthenaFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：十一月三十日，二零一六年十一月三十日

- 編輯時間:2024 年 1 月 3 日, 世界標準時間 19:05
- ARN: arn:aws:iam::aws:policy/AmazonAthenaFullAccess

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAugmentedAIFullAccess

說明：提供執行 Amazon Augmented AI 資源的所有操作的訪問權限 FlowDefinitions，包括 HumanTaskUis 和 HumanLoops。不允許 FlowDefinitions 對公眾人群工作團隊進行創建的訪問。

`AmazonAugmentedAIFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加AmazonAugmentedAIFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一九年十二月三日 16:21 世界標準時間
- 編輯時間：2019 年 12 月 3 日，世界標準時間 16:21
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAugmentedAIHumanLoopFullAccess

描述：提供在上執行所有作業的存取權 HumanLoops。

AmazonAugmentedAIHumanLoopFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAugmentedAIHumanLoopFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**二零一九年十二月三日, 16:20 世界時間
- **編輯時間**：2019 年 12 月 3 日，世界標準時間 16:20
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonAugmentedAIIntegratedAPIAccess

說明：提供執行 Amazon Augmented AI 資源的所有操作的訪問權限 FlowDefinitions，包括 HumanTaskUis 和 HumanLoops。此外，還提供對與 Amazon Augmented AI 整合的服務操作的存取權。

AmazonAugmentedAIIntegratedAPIAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonAugmentedAIIntegratedAPIAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 22 日, 世界標準時間 20:47
- 編輯時間:2020 年 4 月 22 日, 世界標準時間 20:47
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectModerationLabels"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonBedrockFullAccess

說明：提供對 Amazon 基岩的完整存取權限，以及對其所需的相關服務的有限存取權

AmazonBedrockFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonBedrockFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 12 月 6 日，下午 3:47
- 編輯時間：世界標準時間 2023 年 12 月 6 日，下午 3:47
- ARN: arn:aws:iam::aws:policy/AmazonBedrockFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonBedrockReadOnly

說明：提供 Amazon 基岩的唯讀訪問權限

AmazonBedrockReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonBedrockReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 12 月 6 日，下午 3:48
- 編輯時間：世界標準時間 2023 年 12 月 6 日，下午 3:48
- ARN: arn:aws:iam::aws:policy/AmazonBedrockReadOnly

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonBraketFullAccess

說明：透過 AWS Management Console 和 SDK 提供對 Amazon Braket 的完整存取權。也提供對相關服務 (例如 S3、日誌) 的存取。

AmazonBraketFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonBraketFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**:2020 年 8 月 6 日, 世界標準時間 20:12
- **編輯時間**:世界標準時間 2023 年 4 月 19 日, 16:25
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonBraketJobsExecutionPolicy

說明：授予執行 Amazon Braket 任務所需的存取權 AWS 服務 和資源，包括 S3、雲端觀察、IAM 和布拉克特

AmazonBraketJobsExecutionPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonBraketJobsExecutionPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年十一月二十六日, 世界標準時間 19:34
- 編輯時間:2021 年十一月二十八日, 05:34 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonBraketServiceRolePolicy

說明：允許 Amazon Braket 代表您建立和管理 AWS 資源

AmazonBraketServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 8 月 4 日, 世界標準時間 17:12
- 編輯時間:2020 年 8 月 6 日, 世界標準時間 20:10
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeFullAccess

說明：提供透過 Amazon Chime 管理主控台的 AWS Management Console完整存取權。

AmazonChimeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonChimeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 11 月 1 日, 世界標準時間 22:15
- 編輯時間:2020 年十二月十四日, 世界標準時間 21:00
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeReadOnly

說明：透過提供 Amazon Chime 管理主控台的唯讀存取 AWS Management Console權。

`AmazonChimeReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonChimeReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 11 月 1 日，世界標準時間 22 點 4 分
- 編輯時間：2020 年十二月十四日，世界標準時間 20:53
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeSDK

說明：提供對 Amazon Chime SDK 操作的存取

AmazonChimeSDK是AWS 受管理的策略。

使用此政策

您可以附加AmazonChimeSDK至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 2 月 4 日, 21:53 世界標準時間
- 編輯時間：世界標準時間 2023 年 1 月 10 日下午 18:05
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

說明：適用於 Amazon Chime SDK MediaPipelines 服務連結角色的受管政策

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2022 年 4 月 4 日, 上午 22 點 2
- 編輯時間：世界標準時間 2023 年 12 月 8 日，下午 19:14
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeSDKMessagingServiceRolePolicy

說明：允許 Amazon Chime 開發套件簡訊存取 AWS 資源並啟用簡訊功能

AmazonChimeSDKMessagingServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 3 月 3 日，01:43
- 編輯時間：世界標準時間 2023 年 3 月 3 日，01:43
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeServiceRolePolicy

說明：允許存取 Amazon Chime 所使用或管理的 AWS 資源

AmazonChimeServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 9 月 30 日, 世界標準時間 22:25
- 編輯時間：2019 年 9 月 30 日，世界標準時間 22:25
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeTranscriptionServiceLinkedRolePolicy

描述：允許 Amazon Chime 代表您訪問 Amazon Transcribe 和 Amazon Transcribe 醫療

`AmazonChimeTranscriptionServiceLinkedRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 8 月 4 日, 世界標準時間 21:47
- 編輯時間：2021 年 8 月 4 日，世界標準時間 21:47
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeUserManagement

說明：提供使用者透過 Amazon Chime 管理主控台的管理存取 AWS Management Console權。

AmazonChimeUserManagement是AWS 受管理的策略。

使用此政策

您可以附加AmazonChimeUserManagement至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 11 月 1 日, 世界標準時間 22:17
- 編輯時間:2020 年 2 月 18 日, 世界標準時間 19:26
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

說明：適用於 Amazon Chime 的服務連結角色的受管政策 VoiceConnector

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2019 年 9 月 30 日，世界標準時間 22:16
- 編輯時間：世界標準時間 2023 年 4 月 14 日晚上 9 時 49 分

- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCloudDirectoryFullAccess

描述：提供對 Amazon Cloud Directory 服務的完整存取權。

AmazonCloudDirectoryFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCloudDirectoryFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 2 月 25 日，世界標準時間 00:41
- 編輯時間：2017 年 2 月 25 日，世界標準時間 00:41
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCloudDirectoryReadOnlyAccess

說明：提供 Amazon Cloud Directory 服務的唯讀存取權。

AmazonCloudDirectoryReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCloudDirectoryReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 2 月 28 日, 23:42 世界標準時間
- 編輯時間：2017 年 2 月 28 日，世界標準時間 23:42
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCloudWatchEvidentlyFullAccess

描述： CloudWatch 顯而易見地提供對 Amazon 的完全訪問權限。還提供對相關 Amazon S3，Amazon SNS CloudWatch，Amazon 和其他相關服務的訪問。

`AmazonCloudWatchEvidentlyFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonCloudWatchEvidentlyFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 11 月 29 日，世界標準時間下午 3:10
- 編輯時間：2021 年十一月二十九日，世界標準時間 15:10
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCloudWatchEvidentlyReadOnlyAccess

描述： CloudWatch 顯然提供對 Amazon 的只讀訪問權限

AmazonCloudWatchEvidentlyReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCloudWatchEvidentlyReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月二十九日, 世界標準時間 15:08
- 編輯時間：2021 年十一月二十九日，世界標準時間 15:08
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCloudWatchEvidentlyServiceRolePolicy

說明：允許「CloudWatch 明顯服務」代表客戶管理相關 AWS 資源

AmazonCloudWatchEvidentlyServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：2022 年 9 月 13 日，17:25
- 編輯時間：2022 年 9 月 13 日，世界標準時間 17:25
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCloudWatchRUMFullAccess

說明：授予 Amazon CloudWatch RUM 服務的完整存取權限

AmazonCloudWatchRUMFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCloudWatchRUMFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月二十九日，世界標準時間 15:46

- 編輯時間：2021 年十一月二十九日，世界標準時間 15:46
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCloudWatchRUMReadOnlyAccess

說明：授予 Amazon CloudWatch RUM 服務的唯讀權限

AmazonCloudWatchRUMReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCloudWatchRUMReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月二十九日，世界標準時間 15:43
- 編輯時間:2022 年 10 月 28 日, 世界標準時間 18:12
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCloudWatchRUMServiceRolePolicy

說明：授予 Amazon CloudWatch RUM 服務將監控資料發佈到其他相關 AWS 服務的權限

`AmazonCloudWatchRUMServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 11 月 17 日, 23:17
- 編輯時間：世界標準時間 2023 年 2 月 22 日晚上 20:35
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeCatalystFullAccess

描述：提供完全訪問 Amazon CodeCatalyst

AmazonCodeCatalystFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeCatalystFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 4 月 20 日，世界標準時間 16:50
- 編輯時間：世界標準時間 2023 年 4 月 20 日，16:50
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeCatalystReadOnlyAccess

描述：提供對 Amazon 的只讀訪問權限 CodeCatalyst

AmazonCodeCatalystReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeCatalystReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 4 月 20 日，16:49
- 編輯時間：世界標準時間 2023 年 4 月 20 日，16:49
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeCatalystSupportAccess

說明：允許 Amazon CodeCatalyst 代表您建立、更新和解決 AWS Support 案例。

AmazonCodeCatalystSupportAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeCatalystSupportAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 4 月 20 日，下午 12:34
- 編輯時間：世界標準時間 2023 年 4 月 20 日 12:34

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

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeGuruProfilerAgentAccess

描述：提供 Amazon CodeGuru 效能分析工具代理程式所需的存取權。

AmazonCodeGuruProfilerAgentAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeGuruProfilerAgentAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 2 月 5 日, 世界標準時間 22:11
- 編輯時間：2022 年 5 月 5 日，世界標準時間 18:11
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ConfigureAgent",
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeGuruProfilerFullAccess

描述：提供對 Amazon CodeGuru 效能分析工具的完整存取權。

AmazonCodeGuruProfilerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeGuruProfilerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 10:13 世界標準時
- 編輯時間:2020 年 7 月 15 日, 3:23 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeGuruProfilerReadOnlyAccess

說明：提供 Amazon CodeGuru 效能分析工具的唯讀存取權。

AmazonCodeGuruProfilerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeGuruProfilerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 12 月 3 日, 世界標準時間 10:30
- 編輯時間:2020 年 6 月 27 日, 世界標準時間 23:52
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeGuruReviewerFullAccess

說明：授予對 Amazon CodeGuru 審核者的完整存取權限，以及所需相依性的範圍存取權限。

AmazonCodeGuruReviewerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeGuruReviewerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 08:33 世界標準時
- 編輯時間:2020 年 8 月 29 日, 04:16 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeGuruReviewerReadOnlyAccess

描述：提供 Amazon CodeGuru 審核者的唯讀存取權。

AmazonCodeGuruReviewerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeGuruReviewerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 08:48 世界時間
- 編輯時間:2020 年 8 月 29 日, 04:15 世界標準時間
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeGuruReviewerServiceRolePolicy

說明：Amazon CodeGuru 審核者代表您存取資源所需的服務連結角色。

AmazonCodeGuruReviewerServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十二月三日, 05:31 世界標準時
- 編輯時間：2020 年十一月二十七日，世界標準時間 15:09
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeGuruSecurityFullAccess

描述：提供對 Amazon CodeGuru 安全的完整訪問權限。

AmazonCodeGuruSecurityFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeGuruSecurityFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 5 月 9 日, 世界標準時間 21:03
- 編輯時間：世界標準時間 2023 年 5 月 9 日晚上 9 時 03 分
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCodeGuruSecurityScanAccess

描述：提供使用 Amazon CodeGuru 安全掃描所需的存取權。

AmazonCodeGuruSecurityScanAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonCodeGuruSecurityScanAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 5 月 9 日, 世界標準時間 20:54
- 編輯時間：2023 年 5 月 9 日，世界標準時間 20:54
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCognitoDeveloperAuthenticatedIdentities

描述：提供對 Amazon Cognito API 的存取權，以支援從身分驗證後端的開發人員驗證身分。

`AmazonCognitoDeveloperAuthenticatedIdentities`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonCognitoDeveloperAuthenticatedIdentities`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2015 年 3 月 24 日, 17:22
- 編輯時間：2015 年 3 月 24 日，世界標準時間 17:22
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCognitoIdpEmailServiceRolePolicy

說明：允許 Amazon Cognito 使用者集區服務使用您的 SES 身分進行電子郵件傳送

AmazonCognitoIdpEmailServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間**:二零一九年三月二十一日, 21:32 世界標準
- **編輯時間**：2019 年 3 月 21 日，世界標準時間 21:32
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCognitoIdpServiceRolePolicy

說明：啟用 Amazon Cognito 使用者集區所使用或管理的資源存取 AWS 服務 和資源

AmazonCognitoIdpServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 6 月 26 日, 世界標準時間 22:30
- 編輯時間:2020 年 6 月 26 日, 世界標準時間 22:30
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCognitoPowerUser

描述：提供對現有 Amazon Cognito 資源的管理存取權。您需要 AWS 帳戶 管理員權限才能建立新的 Cognito 資源。

AmazonCognitoPowerUser是AWS 受管理的策略。

使用此政策

您可以附加AmazonCognitoPowerUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2015 年 3 月 24 日, 17:14
- 編輯時間：2021 年 6 月 1 日，世界標準時間 17：33
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
```

```
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCognitoReadOnly

說明：提供 Amazon Cognito 資源的唯讀存取權。

AmazonCognitoReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonCognitoReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2015 年 3 月 24 日, 17:06
- 編輯時間：2019 年 8 月 1 日，世界標準時間 19:21
- ARN: arn:aws:iam::aws:policy/AmazonCognitoReadOnly

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCognitoUnAuthedIdentitiesSessionPolicy

描述：此原則定義 Cognito 識別集區未驗證身分所允許的權限集。此原則不適用於作為獨立的權限原則。它被用作防護欄，以防止身份集區中的角色附加過於寬鬆的策略。請勿將此原則附加至任何角色，

因為 Cognito 身分識別服務在建立認證時會自動將其納入為已停用範圍的原則。透過增強型流程暫時存取其他 AWS 資源的權限，現在將由與服務提供的未驗證使用者身分相關聯的角色交集，以及 Cognito 擁有的此受管理策略中提供的權限所定義。

AmazonCognitoUnAuthedIdentitiesSessionPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonCognitoUnAuthedIdentitiesSessionPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 7 月 19 日 23:04
- 編輯時間：世界標準時間 2023 年 7 月 19 日 23:04
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
        "translate:*",
        "transcribe:*",
```

```
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonCognitoUnauthenticatedIdentities

描述：此原則定義 Cognito 識別集區未驗證身分所允許的權限集。這不需要附加至您的未驗證角色，因為 Cognito 身分識別服務會在建立認證時自動將其納入為已設定範圍的原則。透過增強型流程暫時存取其他 AWS 資源的權限，現在將由與服務提供的未驗證使用者身分相關聯的角色交集，以及 Cognito 擁有的此受管理策略中提供的權限所定義。

`AmazonCognitoUnauthenticatedIdentities`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonCognitoUnauthenticatedIdentities`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 2 月 1 日, 22:36
- 編輯時間：世界標準時間 2023 年 2 月 1 日 22:36
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonConnect_FullAccess

描述：此原則的目的是授與使用 [AWS Connect] 資源所需的使用者權限。此原則提供透過 AWS Connect 主控台和公用 API 對 Connect 資源的完整存取

`AmazonConnect_FullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonConnect_FullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年十一月二十日，世界標準時間 19:54
- 編輯時間：世界標準時間 2023 年 3 月 7 日下午 2:49
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonConnectCampaignsServiceLinkedRolePolicy

說明：Amazon Connect 促銷活動服務鏈接角色的政策

AmazonConnectCampaignsServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 9 月 23 日, 世界標準時間 20:54
- 編輯時間：世界標準時間 2023 年 11 月 8 日，16:16
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonConnectReadOnlyAccess

說明：授予 Amazon Connect 您的 AWS 帳戶.

AmazonConnectReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonConnectReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 17 日, 世界標準時間 21:00
- 編輯時間：2019 年 11 月 6 日，世界標準時間 22:10
- ARN: arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonConnectServiceLinkedRolePolicy

描述：允許 Amazon Connect 代表您創建和管理 AWS 資源。

AmazonConnectServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2018 年 9 月 7 日，世界標準時間 00:21
- 編輯時間：世界標準時間：2023 年 11 月 28 日，下午 16 點 05
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid" : "AllowS3ObjectForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*/*"
      ]
    },
    {
      "Sid" : "AllowGetBucketMetadataForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*"
      ]
    },
    {
      "Sid" : "AllowConnectLogGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
      ]
    },
    {
      "Sid" : "AllowListLexBotAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:SearchProfiles",
        "profile:CreateProfile",
        "profile:UpdateProfile",
        "profile:AddProfileKey",
        "profile:ListProfileObjectTypes",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListCalculatedAttributesForProfile",
        "profile:GetDomain",
        "profile:ListIntegrations"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfileObjects",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjects",
        "profile:GetProfileObjectType"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
```

```
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
        "wisdom:UntagResource",
        "wisdom:TagResource",
        "wisdom:CreateSession",
        "wisdom:CreateQuickResponse",
        "wisdom:GetQuickResponse",
        "wisdom:SearchQuickResponses",
        "wisdom:StartImportJob",
        "wisdom:GetImportJob",
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom:DeleteQuickResponse",
        "wisdom:PutFeedback"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
```

```
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetCalculatedAttributeForProfile",
        "profile:CreateCalculatedAttributeDefinition",
        "profile:DeleteCalculatedAttributeDefinition",
        "profile:GetCalculatedAttributeDefinition",
        "profile:UpdateCalculatedAttributeDefinition"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/*"
      ]
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonConnectSynchronizationServiceRolePolicy

說明：允許 Amazon Connect 代表您同步跨區域的 AWS 資源。

`AmazonConnectSynchronizationServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2023 年 10 月 27 日, 世界標準時間 22:38
- 編輯時間：世界標準時間 2023 年 10 月 27 日上午 22 時 38 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonConnectVoiceIDFullAccess

說明：提供對 Amazon Connect 語音 ID 的完整訪問權限

AmazonConnectVoiceIDFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonConnectVoiceIDFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 9 月 26 日，世界標準時間 19:04
- 編輯時間：2021 年 9 月 26 日，世界標準時間 19:04
- ARN: arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneDomainExecutionRolePolicy

描述：Amazon DomainExecutionRole 服務角色 DataZone的預設政策。Amazon 使用此角色 DataZone 來編目、探索、管理、共用和分析 Amazon DataZone 網域中的資料。

`AmazonDataZoneDomainExecutionRolePolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonDataZoneDomainExecutionRolePolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2023 年 9 月 27 日, 21:55
- 編輯時間:2024 年 4 月 1 日, 世界標準時間 19:25
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneEnvironmentRolePermissionsBoundary

說明：Amazon 為環境 DataZone 建立 IAM 角色以執行資料分析動作，並在建立這些角色時使用此政策來定義其許可的界限。

AmazonDataZoneEnvironmentRolePermissionsBoundary是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneEnvironmentRolePermissionsBoundary至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 9 月 11 日 23:38
- 編輯時間：世界標準時間 2023 年 11 月 17 日 23:29
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneFullAccess

說明： DataZone 透過 Amazon 提供對 Amazon 的完整存取權， AWS Management Console 以及對其所需的相關服務的有限存取。

AmazonDataZoneFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 9 月 22 日，晚上 20:06
- 編輯時間：世界標準時間 2024 年 4 月 23 日晚上 9 時 36 分
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneFullUserAccess

描述：提供對 Amazon 的完整存取權 DataZone，但不允許管理網域、使用者或關聯帳戶。

AmazonDataZoneFullUserAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneFullUserAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 9 月 22 日, 21:06
- 編輯時間:2024 年 4 月 1 日, 世界標準時間 19:27
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneGlueManageAccessRolePolicy

說明：該政策授予許可，以允許 Amazon 啟 DataZone 用對資料的發佈和存取授權。

AmazonDataZoneGlueManageAccessRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneGlueManageAccessRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2023 年 9 月 22 日, 20:21

- 編輯時間:2024 年 4 月 1 日, 世界標準時間 19:05
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZonePortalFullAccessPolicy

說明：提供對 Amazon DataZone API 的完整存取權

AmazonDataZonePortalFullAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZonePortalFullAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 3 月 26 日, 18:24
- 編輯時間：世界標準時間 2023 年 3 月 26 日下午 18:24
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZonePreviewConsoleFullAccess

說明：提供 Amazon 預覽版的完整存取權， DataZone 透過 AWS Management Console. 還提供對其他相關服務的選擇訪問權限。

AmazonDataZonePreviewConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZonePreviewConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 3 月 28 日，下午 3:16
- 編輯時間：世界標準時間 2023 年 7 月 13 日下午 18:01
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneProjectDeploymentPermissionsBoundary

說明：Amazon DataZone 建立用於部署資料分析專案的 IAM 角色。 DataZone 建立這些角色時，會使用此原則來定義其權限的界限。

AmazonDataZoneProjectDeploymentPermissionsBoundary是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneProjectDeploymentPermissionsBoundary至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 3 月 21 日，下午 2 時 54 分
- 編輯時間：世界標準時間 2023 年 4 月 4 日，02:48
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneProjectRolePermissionsBoundary

說明：Amazon 為專案 DataZone 建立 IAM 角色以執行資料分析動作，並在建立這些角色時使用此政策來定義其許可的界限。

`AmazonDataZoneProjectRolePermissionsBoundary`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonDataZoneProjectRolePermissionsBoundary`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 3 月 21 日, 02:51 世界標準時間
- 編輯時間：世界標準時間 2023 年 3 月 21 日，02:51
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

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

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

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

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

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneRedshiftGlueProvisioningPolicy

描述：Amazon DataZone 是一種資料管理服務，可讓您編目、探索、控管、共用和分析資料。使用 Amazon DataZone，您可以跨帳戶和支援的區域共用和存取資料。Amazon DataZone 簡化了您跨 AWS 服務的體驗，包括但不限於 Amazon Redshift，Amazon Athena， AWS Glue 和 AWS Lake Formation。

`AmazonDataZoneRedshiftGlueProvisioningPolicy`是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneRedshiftGlueProvisioningPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 9 月 22 日, 20:19
- 編輯時間：世界標準時間 2024 年 3 月 12 日，16:44
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

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

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

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

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

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

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

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneRedshiftManageAccessRolePolicy

說明：此政策授予 Amazon DataZone 許可，將 Amazon Redshift 數據發佈到目錄。它還授予 Amazon DataZone 許可，以授予目錄中亞馬遜 Redshift 或亞馬遜 Redshift 無伺服器已發佈資產的存取權或撤銷存取權。

`AmazonDataZoneRedshiftManageAccessRolePolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonDataZoneRedshiftManageAccessRolePolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2023 年 9 月 22 日, 20:15
- 編輯時間：世界標準時間 2023 年 11 月 16 日上午 22 時 4 分
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

描述：該 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 政策是在 Amazon 佈建的 SageMaker 環境中建立的執行角色上允許的許可清單 DataZone。

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 23 日, 世界標準時間 23:01
- 編輯時間:2024 年 5 月 8 日, 02:03 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : [
        "*"
      ]
```

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

```
      "Effect" : "Allow",
      "Action" : [
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:ListJobs",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:GetTable",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
        "glue:GetDatabase"
      ],
```

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

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

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

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

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

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

```
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
```

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

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

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

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

```
        "tag:GetResources",
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneSageMakerManageAccessRolePolicy

描述：該 AmazonDataZoneSageMakerManageAccessRolePolicy 政策授予 Amazon 所需 DataZone 的許可，以授予使用者對 SageMaker 環境中各種資源的存取權。

AmazonDataZoneSageMakerManageAccessRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneSageMakerManageAccessRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 23 日, 世界標準時間 23:34
- 編輯時間：世界標準時間 2024 年 4 月 23 日 23:34
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDataZoneSageMakerProvisioningRolePolicy

說明：該 AmazonDataZoneSageMakerProvisioningRolePolicy 政策授予 Amazon DataZone 與 Amazon SageMaker 互操作所需的許可。

`AmazonDataZoneSageMakerProvisioningRolePolicy`是AWS 受管理的策略。

使用此政策

您可以附加AmazonDataZoneSageMakerProvisioningRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 23 日, 世界標準時間 23:32
- 編輯時間：世界標準時間 2024 年 4 月 23 日 23:32
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDetectiveFullAccess

說明：提供 Amazon Detective 服務的完整存取權限，以及主控台 UI 相依性的範圍存取

AmazonDetectiveFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDetectiveFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 30 日, 世界標準時間 17:57
- 編輯時間:2023 年 5 月 17 日, 世界標準時間 19:39
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDetectiveInvestigatorAccess

描述：為調查人員提供 Amazon Detective 服務的存取權，以及主控台 UI 相依性的範圍存取權限。本政策允許潛入 Detective 以進行調查，並限制對 Guardduty 的寫入權限。

AmazonDetectiveInvestigatorAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDetectiveInvestigatorAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 1 月 17 日, 世界標準時間 15:24
- 編輯時間:2023 年 11 月 27 日, 3:13 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDetectiveMemberAccess

說明：提供成員對 Amazon Detective 服務的存取權，以及主控台 UI 相依性的範圍存取權限。

AmazonDetectiveMemberAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDetectiveMemberAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 1 月 17 日, 下午 3:16
- 編輯時間：世界標準時間 2023 年 1 月 17 日下午 3:16
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDetectiveOrganizationsAccess

描述：提供 Organizations 存取權以管理 Amazon Detective 的委派管理員，以及對主控台 UI 相依性的範圍存取權限。這也授予為 Detective 建立服務連結角色的權限。

`AmazonDetectiveOrganizationsAccess`是AWS 受管理的策略。

使用此政策

您可以附加AmazonDetectiveOrganizationsAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 3 月 2 日, 下午 3:20
- 編輯時間：世界標準時間 2023 年 3 月 2 日下午 3:20
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDetectiveServiceLinkedRolePolicy

描述：允許 Amazon Detective 代表您撥打服務電話

`AmazonDetectiveServiceLinkedRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年十一月十八日, 世界標準時間 19:47
- 編輯時間：2021 年十一月十八日，世界標準時間 19:47
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDevOpsGuruConsoleFullAccess

說明：此原則會授與 DevOps Guru 主控台的完整存取權。

AmazonDevOpsGuruConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDevOpsGuruConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年十二月十七日, 世界標準時間 18:43
- 編輯時間：2022 年 8 月 25 日，世界標準時間 18:18
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDevOpsGuruFullAccess

描述：提供對 Amazon DevOps 大師的完全訪問權限。

AmazonDevOpsGuruFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDevOpsGuruFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 12 月 1 日, 世界標準時間 16:38
- 編輯時間：2022 年 8 月 25 日，世界標準時間 18:23
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDevOpsGuruOrganizationsAccess

描述：提供在組織內啟用和管理 Amazon DevOps Guru 的存取權。

AmazonDevOpsGuruOrganizationsAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDevOpsGuruOrganizationsAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月十五日，世界標準時間 23:50
- 編輯時間：2021 年十一月十五日，世界標準時間 23:50
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDevOpsGuruReadOnlyAccess

說明：提供 Amazon DevOps Guru 主控台的唯讀存取權。

AmazonDevOpsGuruReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDevOpsGuruReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 12 月 1 日, 16:34 世界標準時間
- 編輯時間：2022 年 8 月 25 日，世界標準時間 18:11
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDevOpsGuruServiceRolePolicy

說明：Amazon DevOpsGuru 存取資源所需的服務連結角色。

AmazonDevOpsGuruServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年十二月 1 日, 上午 10:24 世界標準時間
- 編輯時間：世界標準時間 2023 年 1 月 10 日下午 2:36
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDMSCloudWatchLogsRole

說明：提供將 DMS 複寫日誌上傳到客戶帳戶中的 cloudwatch 日誌的存取權。

AmazonDMSCloudWatchLogsRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonDMSCloudWatchLogsRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2016 年 1 月 7 日, 23:44 世界標準時間
- 編輯時間:2023 年 5 月 23 日, 世界標準時間 21:32
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDMSRedshiftS3Role

描述：提供管理 DMS Redshift 端點 S3 設定的存取權。

AmazonDMSRedshiftS3Role是AWS 受管理的策略。

使用此政策

您可以附加AmazonDMSRedshiftS3Role至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一六年四月二十日, 17:05 世界標準時

- 編輯時間:2019 年 7 月 8 日, 世界標準時間 18:19
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDMSVPCManagementRole

描述：提供管理客戶組態管理 VPC 設定的 AWS 存取權

AmazonDMSVPCManagementRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonDMSVPCManagementRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:十一月十八日, 世界標準時間 16:33
- 編輯時間：2016 年 5 月 23 日，世界標準時間 16:29
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDocDB-ElasticServiceRolePolicy

描述：允許亞馬遜文檔 DB 彈性代表您管理 AWS 資源。

AmazonDocDB-ElasticServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：二零二二年十一月三十日，世界標準時間
- 編輯時間：二 ○ 二二年十一月三十日，世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDocDBConsoleFullAccess

說明：提供完整的存取權以管理 Amazon DocumentDB 與 MongoDB 相容性，使用. AWS Management Console請注意，此政策還授予在帳戶內所有 SNS 主題上發佈的完整存取權、建立和編輯 Amazon EC2 執行個體和 VPC 組態的許可、在 Amazon KMS 上檢視和列出金鑰的許可，以及對 Amazon RDS 和 Amazon Neptune 的完整存取權限。

AmazonDocDBConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDocDBConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年一月九日, 世界標準時間 20:37
- 編輯時間：二 ○ 二二年十一月三十日，世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
```

```
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
```

```
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
```

```
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDocDBElasticFullAccess

說明：提供對 Amazon DocumentDB 彈性叢集的完整存取權，以及其相依性的其他必要許可，包括 EC2 SecretsManager、KMS CloudWatch 和 IAM。

AmazonDocDBElasticFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDocDBElasticFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 6 月 5 日，下午 13:51
- 編輯時間:2023 年 6 月 21 日, 世界標準時間 18:05
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDocDBElasticReadOnlyAccess

說明：提供 Amazon 文件資料庫彈性和指標的唯讀存取權。 CloudWatch

AmazonDocDBElasticReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDocDBElasticReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 6 月 8 日，下午 2:37

- 編輯時間：世界標準時間 2023 年 6 月 21 日，16:57
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDocDBFullAccess

說明：提供具有 MongoDB 相容性的亞馬遜文件資料庫的完整存取權。請注意，此政策還授予對帳戶內所有 SNS 主題進行發佈的完整存取權，以及對 Amazon RDS 和 Amazon Neptune 的完整存取權。

AmazonDocDBFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDocDBFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 1 月 9 日, 世界標準時間 20:21
- 編輯時間：2019 年 1 月 9 日，世界標準時間 20:21
- ARN: arn:aws:iam::aws:policy/AmazonDocDBFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
```

```
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
```

```
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDocDBReadOnlyAccess

說明：提供具有 MongoDB 相容性的亞馬遜文件資料庫的唯讀存取權。請注意，此政策還授予對 Amazon RDS 和亞馬 Amazon Neptune 資源的存取權。

AmazonDocDBReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDocDBReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 1 月 9 日, 世界標準時間 20:30

- **編輯時間**：2019 年 1 月 9 日，世界標準時間 20:30
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDRSVPCManagement

說明：提供管理 Amazon 受管客戶組態之 VPC 設定的存取權

AmazonDRSVPCManagement是AWS 受管理的策略。

使用此政策

您可以附加AmazonDRSVPCManagement至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2015 年 9 月 2 日，世界標準時間 00:09
- 編輯時間：2015 年 9 月 2 日，世界標準時間 00:09
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDynamoDBFullAccess

說明：可透過. AWS Management Console

AmazonDynamoDBFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDynamoDBFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**2015 年 2 月 6 日, 18:40 世界標準時間
- **編輯時間**：2021 年 1 月 29 日，世界標準時間 17：38
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

政策版本

策略版本：v15(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDynamoDBFullAccesswithDataPipeline

說明：此原則位於淘汰路徑上。請參閱說明文件以取得指引：https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html。提供對 Amazon DynamoDB 的完整存取權，包 Data Pipeline 過 AWS . AWS Management Console

AmazonDynamoDBFullAccesswithDataPipeline是AWS 受管理的策略。

使用此政策

您可以附加AmazonDynamoDBFullAccesswithDataPipeline至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間:二零一五年十一月十二日, 02:17 世界標準
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonDynamoDBReadOnlyAccess

說明：提供 Amazon DynamoDB 的唯讀存取權，透過. AWS Management Console

AmazonDynamoDBReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonDynamoDBReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2024 年 3 月 20 日下午 3:45
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEBSCSIDriverPolicy

說明：允許 CSI 駕駛員服務帳戶代表您撥打相關服務（例如 EC2）的 IAM 政策。

AmazonEBSCSIDriverPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEBSCSIDriverPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間（世界標準時間）4 月 4 日
- 編輯時間：2022 年十一月十八日，世界標準時間 14:42
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2ContainerRegistryFullAccess

說明：提供對 Amazon ECR 資源的管理存取

AmazonEC2ContainerRegistryFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2ContainerRegistryFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一五年十二月二十一日, 下午 17 點 06
- 編輯時間：2020 年 12 月 5 日，世界標準時間 00:04
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2ContainerRegistryPowerUser

說明：提供對 Amazon EC2 容器登錄儲存庫的完整存取權，但不允許刪除儲存庫或政策變更。

AmazonEC2ContainerRegistryPowerUser是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2ContainerRegistryPowerUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一五年十二月二十一日, 下午 17 點 05
- 編輯時間：2019 年 12 月 10 日，世界標準時間 20:48
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2ContainerRegistryReadOnly

說明：提供 Amazon EC2 容器登錄儲存庫的唯讀存取權。

`AmazonEC2ContainerRegistryReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonEC2ContainerRegistryReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一五年十二月二十一日，下午 17 點 4
- 編輯時間：2019 年 12 月 10 日，世界標準時間 20:56
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2ContainerServiceAutoscaleRole

說明：為 Amazon EC2 容器服務啟用任務自動調度資源的政策

AmazonEC2ContainerServiceAutoscaleRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2ContainerServiceAutoscaleRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2016 年 5 月 12 日, 23:25 世界標準時間
- 編輯時間:2018 年 2 月 5 日, 世界標準時間 19:15
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2ContainerServiceEventsRole

說明：啟用 EC2 容器服務 CloudWatch 事件的政策

AmazonEC2ContainerServiceEventsRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2ContainerServiceEventsRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 5 月 30 日, 世界標準時間 16:51
- 編輯時間：世界標準時間 2023 年 3 月 6 日 22:25
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2ContainerServiceforEC2Role

說明：適用於 Amazon EC2 Amazon EC2 Container Service 角色的預設政策。

AmazonEC2ContainerServiceforEC2Role是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2ContainerServiceforEC2Role至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2015 年 3 月 19 日, 18:45
- 編輯時間：世界標準時間 2023 年 3 月 6 日 22:19
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2ContainerServiceRole

說明：Amazon ECS 服務角色的預設政策。

AmazonEC2ContainerServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2ContainerServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 4 月 9 日, 16:14 世界標準時間
- 編輯時間：2016 年 8 月 11 日，世界標準時間 13:08
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2FullAccess

說明：提供完整的 Amazon EC2 存取權，透過 AWS Management Console.

AmazonEC2FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間:2018 年十一月二十七日, 02:16 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonEC2FullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2ReadOnlyAccess

說明：提 Amazon EC2 過 AWS Management Console.

AmazonEC2ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2024 年 2 月 14 日下午 18:43
- ARN: arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2RoleforAWSCodeDeploy

說明：提供 S3 儲存貯體的 EC2 存取權以下載修訂版本。EC2 執行個體上的 CodeDeploy 代理程式需要此角色。

AmazonEC2RoleforAWSCodeDeploy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2RoleforAWSCodeDeploy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 5 月 19 日, 18:10 世界標準時間
- 編輯時間：2017 年 3 月 20 日，世界標準時間 17:14
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2RoleforAWSCodeDeployLimited

說明：提供 EC2 對 S3 儲存貯體的有限存取權限以下載修訂版本。EC2 執行個體上的 CodeDeploy 代理程式需要此角色。

AmazonEC2RoleforAWSCodeDeployLimited是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2RoleforAWSCodeDeployLimited至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 8 月 24 日, 世界標準時間 17:55
- 編輯時間：2022 年一月二十日，世界標準時間 21:37
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2RoleforDataPipelineRole

說明：適用於 Data Pipeline 服務角色之 Amazon EC2 角色的預設政策。

`AmazonEC2RoleforDataPipelineRole`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonEC2RoleforDataPipelineRole`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：世界標準時間 2016 年 2 月 22 日 17:24
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2RoleforSSM

說明：這個原則很快就會被淘汰。請使用 AmazonSSM ManagedInstanceCore 政策在 EC2 執行個體上啟用 AWS Systems Manager 服務核心功能。如需更多資訊，請setup-instance-profile參閱 https://docs.aws.amazon.com/systems-manager/latest/userguide/

AmazonEC2RoleforSSM是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2RoleforSSM至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 5 月 29 日, 世界標準時間 17:48
- 編輯時間：2019 年 1 月 24 日，世界標準時間 19:20
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2RolePolicyForLaunchWizard

說明：適用於 EC2 之 Amazon LaunchWizard 服務角色的受管政策

AmazonEC2RolePolicyForLaunchWizard是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2RolePolicyForLaunchWizard至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月十三日, 08:05 世界標準
- 編輯時間：2022 年 5 月 16 日，世界標準時間 21:16
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2SpotFleetAutoscaleRole

說明：為 Amazon EC2 競價型叢集啟用自動調度資源的政策

AmazonEC2SpotFleetAutoscaleRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2SpotFleetAutoscaleRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2016 年 8 月 19 日, 世界標準時間 18:27
- 編輯時間：2019 年 2 月 18 日，世界標準時間 19:17
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEC2SpotFleetTaggingRole

說明：允許 EC2 Spot 叢集代表您請求、終止和標記 Spot 執行個體。

AmazonEC2SpotFleetTaggingRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonEC2SpotFleetTaggingRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 6 月 29 日, 世界標準時間 18:19
- 編輯時間:2020 年 4 月 23 日, 世界標準時間 19:30
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonECS_FullAccess

描述：提供對 Amazon ECS 資源的管理存取權，並透過存取其他 AWS 服務資源 (包括 VPC、Auto Scaling 群組和堆疊) 來啟用 ECS 功能。 CloudFormation

AmazonECS_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonECS_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一七年十一月七日 21:36 世界標準時間
- 編輯時間：世界標準時間 2023 年 1 月 4 日 16:26
- ARN: arn:aws:iam::aws:policy/AmazonECS_FullAccess

政策版本

策略版本：v20(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

描述：提供私人憑證授權單位、機 AWS 密管理員及其他代表您管理 ECS 服務 Connect TLS 功能 AWS 服務 所需的管理存取權。

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2024 年 1 月 19 日, 世界標準時間 20:08
- 編輯時間：世界標準時間 2024 年 1 月 19 日晚上 20:08
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonECSInfrastructureRolePolicyForVolumes

描述：提供存取代表您管理與 ECS 工作負載關聯的磁碟區所需的其他 AWS 服務資源。

AmazonECSInfrastructureRolePolicyForVolumes是AWS 受管理的策略。

使用此政策

您可以附加AmazonECSInfrastructureRolePolicyForVolumes至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 2024 年 1 月 10 日, 22:56
- 編輯時間：世界標準時間 2024 年 1 月 10 日 22:56
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonECSServiceRolePolicy

說明：使 Amazon ECS 能夠管理叢集的政策。

AmazonECSServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 10 月 14 日, 01:18 世界標準時間
- 編輯時間：世界標準時間 2023 年 12 月 4 日下午 19:32
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonECSTaskExecutionRolePolicy

說明：提供對執行 Amazon ECS 任 AWS 務所需的其他服務資源的存取

AmazonECSTaskExecutionRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonECSTaskExecutionRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年十一月十六日, 世界標準時間 18:48
- 編輯時間：2017 年十一月十六日，世界標準時間 18:48

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

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEFSCSIDriverPolicy

說明：提供 EFS 資源的管理存取權，以及 EC2 的讀取存取權

AmazonEFSCSIDriverPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEFSCSIDriverPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2023 年 7 月 25 日, 20:10
- 編輯時間：世界標準時間 2023 年 7 月 25 日晚上 20:10
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKS_CNI_Policy

說明：此政策為 Amazon VPC CNI 外掛程式 (amazon-vpc-cni-k8 秒) 提供修改 EKS 工作者節點上的 IP 位址組態所需的許可。此權限集允許 CNI 代表您列出、描述和修改彈性網路介面。有關 AWS VPC CNI 插件的更多信息，請點擊這裡：https://github.com/aws/ 8 秒 amazon-vpc-cni-k

AmazonEKS_CNI_Policy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEKS_CNI_Policy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 27 日, 世界標準時間 21:07
- 編輯時間：世界標準時間 2024 年 3 月 4 日，20:20
- ARN: arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSClusterPolicy

描述：此原則提供 Kubernetes 代表您管理資源所需的權限。Kubernetes 需要 EC2：CreateTags 許可才能在 EC2 資源上放置識別資訊，包括但不限於執行個體、安全群組和彈性網路界面。

AmazonEKSClusterPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEKSClusterPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 27 日, 世界標準時間 21:06
- 編輯時間：世界標準時間 2023 年 2 月 7 日下午 17 時 33 分
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSConnectorServiceRolePolicy

說明：此政策允許 Amazon EKS 管理 EKS 連接器的 AWS 資源

AmazonEKSConnectorServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 9 月 4 日, 世界標準時間 20:31
- 編輯時間：2021 年 9 月 4 日，世界標準時間 20:31
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSFargatePodExecutionRolePolicy

說明：可讓您存取在 AWS Fargate 上執行 Amazon EKS 網繭所需的其他 AWS 服務資源

AmazonEKSFargatePodExecutionRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEKSFargatePodExecutionRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月二十二日, 04:34 世界標
- 編輯時間:2019 年十一月二十二日, 04:34 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSForFargateServiceRolePolicy

說明：此政策授予 Amazon EKS 執行遠端任務的必要許可

AmazonEKSForFargateServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月二十二日, 04:36 世界標
- 編輯時間:2019 年 11 月 22 日, 04:36 世界標準時間
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSLocalOutpostClusterPolicy

說明：此原則提供權限給在您帳戶中執行的 EKS 本機叢集的控制平面執行個體，以代表您管理資源。

AmazonEKSLocalOutpostClusterPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEKSLocalOutpostClusterPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 24 日，世界標準時間 21:56
- 編輯時間：2022 年 10 月 17 日，世界標準時間 16:02
- ARN: arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSLocalOutpostServiceRolePolicy

說明：允許 Amazon EKS 本地代表您撥打 AWS 服務。

AmazonEKSLocalOutpostServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2022 年 8 月 23 日，世界標準時間 21:53
- 編輯時間：2022 年 10 月 24 日，世界標準時間下午 16:24
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSServicePolicy

描述：此政策允許 Amazon Elastic Container Service for Kubernetes 建立和管理必要的資源來操作 EKS 叢集。

AmazonEKSServicePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEKSServicePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 27 日, 世界標準時間 21:08
- 編輯時間:2020 年 5 月 27 日, 世界標準時間 19:27
- ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSServiceRolePolicy

說明：Amazon EKS 代表您呼叫 AWS 服務所需的服務連結角色。

AmazonEKSServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 2 月 21 日, 世界標準時間 20:10

- 編輯時間:2020 年 5 月 27 日, 世界標準時間 19:30
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSVPCResourceController

描述：VPC 資源控制器用於管理背景工作節點的 ENI 和 IP 的政策。

AmazonEKSVPCResourceController是AWS 受管理的策略。

使用此政策

您可以附加AmazonEKSVPCResourceController至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**：2020 年 8 月 12 日，世界標準時間 00:55
- **編輯時間**：2020 年 8 月 12 日，世界標準時間 00:55
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEKSWorkerNodePolicy

說明：此政策允許 Amazon EKS 工作者節點連接到 Amazon EKS 叢集。

AmazonEKSWorkerNodePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonEKSWorkerNodePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 27 日, 世界標準時間 21:09
- 編輯時間：世界標準時間：2023 年 11 月 27 日凌時 6 分
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElastiCacheFullAccess

描述：提供完全訪問 Amazon ElastiCache 通過 AWS Management Console.

AmazonElastiCacheFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElastiCacheFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間

- 編輯時間：世界標準時間：2023 年十一月二十八日，03:49
- ARN: arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElastiCacheReadOnlyAccess

說明：提供 ElastiCache 透過 Amazon 的唯讀存取權限 AWS Management Console。

AmazonElastiCacheReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElastiCacheReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**2015 年 2 月 6 日, 18:40 世界標準時間
- **編輯時間：**2015 年 2 月 6 日，世界標準時間 18:40
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticContainerRegistryPublicFullAccess

說明：提供 Amazon ECR 公用資源的管理存取權

`AmazonElasticContainerRegistryPublicFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticContainerRegistryPublicFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月 1 日, 世界標準時間 17:25
- 編輯時間:2020 年十二月 1 日, 世界標準時間 17:25
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticContainerRegistryPublicPowerUser

說明：提供對 Amazon ECR 公用儲存庫的完整存取權，但不允許刪除儲存庫或變更政策。

AmazonElasticContainerRegistryPublicPowerUser是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticContainerRegistryPublicPowerUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 12 月 1 日, 16:16 世界標準時間
- 編輯時間：2020 年 12 月 1 日，世界標準時間 16:16
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticContainerRegistryPublicReadOnly

說明：提供 Amazon ECR 公用儲存庫的唯讀存取權。

AmazonElasticContainerRegistryPublicReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticContainerRegistryPublicReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二零年十二月 1 日, 17 世界標準時間

- 編輯時間:2020 年十二月 1 日, 世界標準時間 17:27
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticFileSystemClientFullAccess

說明：提供根用戶端存取 Amazon EFS 檔案系統

AmazonElasticFileSystemClientFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticFileSystemClientFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 1 月 13 日, 世界標準時間 16:27
- 編輯時間:2020 年 1 月 13 日, 世界標準時間 16:27
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticFileSystemClientReadOnlyAccess

說明：提供 Amazon EFS 檔案系統的唯讀用戶端存取權

`AmazonElasticFileSystemClientReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonElasticFileSystemClientReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 1 月 13 日, 世界標準時間 16:24
- 編輯時間：2020 年 1 月 13 日，世界標準時間 16:24
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticFileSystemClientReadWriteAccess

說明：提供對 Amazon EFS 檔案系統的讀取和寫入用戶端存取

`AmazonElasticFileSystemClientReadWriteAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonElasticFileSystemClientReadWriteAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 1 月 13 日, 世界標準時間 16:21
- 編輯時間:2020 年 1 月 13 日, 世界標準時間 16:21
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticFileSystemFullAccess

說明：提供完整的 Amazon EFS 存取權，透過 AWS Management Console.

AmazonElasticFileSystemFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticFileSystemFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**2015 年 5 月 27 日, 16:22 世界標準時間
- **編輯時間:**2023 年 11 月 28 日, 世界標準時間 16:53
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticFileSystemReadOnlyAccess

說明：提供 Amazon EFS 的唯讀存取權，透過 AWS Management Console.

AmazonElasticFileSystemReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticFileSystemReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 5 月 27 日, 16:25 世界標準時間
- 編輯時間：2022 年 1 月 10 日，世界標準時間 18:53
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticFileSystemServiceRolePolicy

說明：允許 Amazon Elastic File System 代表您管理 AWS 資源

AmazonElasticFileSystemServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月五日, 16:52 世界標準時
- 編輯時間：2022 年 1 月 10 日，世界標準時間 19:27
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticFileSystemsUtils

說明：允許客戶使用 AWS Systems Manager 在其 EC2 執行個體上自動管理 Amazon EFS 公用程式 (amazon-efs-utils) 套件，並用 CloudWatchLog 於取得 EFS 檔案系統掛載成功/失敗通知。

AmazonElasticFileSystemsUtils是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticFileSystemsUtils至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 9 月 29 日，世界標準時間 15:16
- 編輯時間：2020 年 9 月 29 日，世界標準時間 15:16
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticMapReduceEditorsRole

描述：Amazon 彈性 MapReduce 編輯器服務角色的預設政策。

AmazonElasticMapReduceEditorsRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticMapReduceEditorsRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年十一月十六日, 世界標準時間 21:55
- 編輯時間：世界標準時間 2023 年 2 月 9 日 22:39
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticMapReduceforAutoScalingRole

描述：Amazon 彈性 MapReduce Auto Scaling。允許 Auto Scaling 從 EMR 叢集新增和移除執行個體的角色。

AmazonElasticMapReduceforAutoScalingRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticMapReduceforAutoScalingRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一六年十一月十八日, 01:09 世界標準
- 編輯時間:十一月十八日, 二零一六年十一月十八日
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticMapReduceforEC2Role

描述：適用於 EC2 服務角色的 Amazon 彈性 MapReduce 預設政策。

AmazonElasticMapReduceforEC2Role是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticMapReduceforEC2Role至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2017 年 8 月 11 日，世界標準時間 23:57

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticMapReduceFullAccess

說明：此原則位於淘汰路徑上。請參閱文檔以獲取指導：ManagementGuideemr-managed-iam-policieshttps://docs.aws.amazon.com/emr/latest/ 提供對 Amazon 彈性 MapReduce 及其所需的基礎服務 (例如 EC2 和 S3) 的完整存取權

AmazonElasticMapReduceFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticMapReduceFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2019 年 10 月 11 日，世界標準時間 15:19
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticMapReducePlacementGroupPolicy

說明：允許 EMR 建立、描述和刪除 EC2 置放群組的政策。

AmazonElasticMapReducePlacementGroupPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticMapReducePlacementGroupPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 9 月 29 日，世界標準時間 00:37
- 編輯時間：2020 年 9 月 29 日，世界標準時間 00:37
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticMapReduceReadOnlyAccess

說明：提供 Amazon 彈性的唯讀存取權限， MapReduce 透過 AWS Management Console.

AmazonElasticMapReduceReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticMapReduceReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間

- 編輯時間:2020 年 7 月 29 日, 世界標準時間 23:14
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticMapReduceRole

說明：此原則位於淘汰路徑上。請參閱文檔以獲取指導：https://docs.aws.amazon.com/emr/latest/ManagementGuide emr-managed-iam-policies。Amazon 彈性 MapReduce 服務角色的預設政策。

AmazonElasticMapReduceRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticMapReduceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間:2020 年 6 月 24 日, 世界標準時間 22:24
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticsearchServiceRolePolicy

說明：允許 Amazon Elasticsearch Service 代表您存取其他 AWS 服務，例如 EC2 聯網 API。

AmazonElasticsearchServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 7 月 7 日, 00:15 世界標準時間
- 編輯時間:2023 年 10 月 23 日, 06:58 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticTranscoder_FullAccess

說明：授予使用者對 Elastic Transcoder 的完整存取權，以及完整 Elastic Transcoder 功能所需的相關服務存取權。

AmazonElasticTranscoder_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticTranscoder_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 4 月 27 日, 世界標準時間 18:59
- 編輯時間：2019 年 6 月 10 日，世界標準時間 22:51
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticTranscoder_JobsSubmitter

說明：授予使用者變更預設集、提交工作和檢視 Elastic Transcoder 設定的權限。此政策還授予對使用彈性轉碼控制台（包括 S3、IAM 和 SNS）所需的一些其他服務的某些唯讀存取權。

AmazonElasticTranscoder_JobsSubmitter是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticTranscoder_JobsSubmitter至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 7 日, 21:12 世界標準時間
- 編輯時間：2019 年 6 月 10 日，世界標準時間 22:49
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticTranscoder_ReadOnlyAccess

說明：授予使用者 Elastic Transcoder 的唯讀存取權，並列出相關服務的存取權。

AmazonElasticTranscoder_ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticTranscoder_ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 7 日, 世界標準時間 21:09
- 編輯時間：2019 年 6 月 10 日，世界標準時間 22:48

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

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonElasticTranscoderRole

描述：Amazon 彈性轉碼器服務角色的預設政策。

AmazonElasticTranscoderRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonElasticTranscoderRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2019 年 6 月 13 日，世界標準時間 22:48
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEMRCleanupPolicy

描述：如果 EMR 服務角色喪失該能力，則允許 EMR 終止和刪除 AWS EC2 資源所需的動作。

AmazonEMRCleanupPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年 9 月 26 日，世界標準時間 23:54
- 編輯時間：2020 年 9 月 29 日，世界標準時間 21:11
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEMRContainersServiceRolePolicy

說明：允許存取執行 Amazon EMR 所需的其他 AWS 服務資源

AmazonEMRContainersServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2020 年十二月九日，世界標準時間 00:38
- 編輯時間：世界標準時間 2023 年 3 月 10 日晚上 22 時 58 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEMRFullAccessPolicy_v2

說明：提供對 Amazon EMR 的完整訪問權限

AmazonEMRFullAccessPolicy_v2是AWS 受管理的策略。

使用此政策

您可以附加AmazonEMRFullAccessPolicy_v2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 3 月 12 日, 凌晨 01 時 50 分
- 編輯時間：世界標準時間 7 月 28 日，下午 4 時 4 分
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEMRReadOnlyAccessPolicy_v2

說明：提供 Amazon EMR 和相關 CloudWatch 指標的唯讀存取權。

AmazonEMRReadOnlyAccessPolicy_v2是AWS 受管理的策略。

使用此政策

您可以附加AmazonEMRReadOnlyAccessPolicy_v2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 3 月 12 日, 01:39 世界標準時間
- 編輯時間:2023 年 8 月 2 日, 世界標準時間 19:15
- ARN: arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEMRServerlessServiceRolePolicy

說明：允許存取執行 Amazon 無伺 AWS 服器所需的其他服務資源

AmazonEMRServerlessServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2022 年 5 月 20 日, 世界標準時間 23:15
- 編輯時間：世界標準時間 2024 年 1 月 25 日 18:21
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEMRServicePolicy_v2

說明：此政策用於 Amazon EMR 服務角色，不應用於帳戶中的任何其他 IAM 使用者或角色。此原則授與建立和管理 EMR 相關資源的權限，以及 EMR 叢集作業所需的相關服務。

AmazonEMRServicePolicy_v2是AWS 受管理的策略。

使用此政策

您可以附加AmazonEMRServicePolicy_v2至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年 3 月 12 日, 世界標準時間 1:11

- 編輯時間:2024 年 5 月 2 日, 世界標準時間 18:43
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonESCognitoAccess

描述：提供對 Amazon Cognito 組態服務的有限存取權限。

AmazonESCognitoAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonESCognitoAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 2 月 28 日, 世界標準時間 22:29
- 編輯時間：2021 年十二月二十日，世界標準時間 14:04
- ARN: arn:aws:iam::aws:policy/AmazonESCognitoAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonESFullAccess

描述：提供對 Amazon ES 組態服務的完整存取權。

AmazonESFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonESFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一五年十月一日, 19:14 世界標準時間
- 編輯時間:2015 年 10 月 1 日, 世界標準時間 19:14
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonESReadOnlyAccess

說明：提供對 Amazon ES 組態服務的唯讀存取權。

AmazonESReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonESReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一五年十月一日, 19:18 世界標準時間
- 編輯時間:二零一八年十月三日, 3:32 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonESReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgeApiDestinationsServiceRolePolicy

描述：允 EventBridge 許代表您存取秘密管理員資源。

AmazonEventBridgeApiDestinationsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 2 月 11 日, 世界標準時間 20:52
- 編輯時間：2021 年 2 月 11 日，世界標準時間 20:52
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgeFullAccess

描述：提供對 Amazon 的完全訪問權限 EventBridge。

AmazonEventBridgeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEventBridgeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 7 月 11 日, 世界標準時間 14:08
- 編輯時間：世界標準時間 2022 年 12 月 1 日下午 5 點
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgePipesFullAccess

描述：提供對 Amazon EventBridge 管道的完整訪問權限。

AmazonEventBridgePipesFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEventBridgePipesFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間（世界標準時間）
- 編輯時間：世界標準時間：2022 年十二月一日下午 17 時
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgePipesOperatorAccess

描述：提供對 Amazon EventBridge 管道的唯讀和操作員 (停止和開始執行管道的功能) 存取權。

AmazonEventBridgePipesOperatorAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEventBridgePipesOperatorAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間（世界標準時間）
- 編輯時間：世界標準時間 2022 年 12 月 1 日下午 17 時 4 分
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgePipesReadOnlyAccess

描述：提供 Amazon EventBridge 管道的唯讀存取權。

AmazonEventBridgePipesReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEventBridgePipesReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間（世界標準時間）
- 編輯時間：世界標準時間 2022 年 12 月 1 日下午 17 時 4 分
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgeReadOnlyAccess

描述：提供對 Amazon 的只讀訪問權限 EventBridge。

`AmazonEventBridgeReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonEventBridgeReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 7 月 11 日, 世界標準時間 13:59
- 編輯時間：世界標準時間：2022 年 12 月 1 日，下午 5 時
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgeSchedulerFullAccess

描述： AmazonEventBridgeSchedulerFullAccess 受管理的策略授與使用排程器和 EventBridge 排程群組的所有「排程器」動作的權限。

AmazonEventBridgeSchedulerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEventBridgeSchedulerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零二二年十一月十日，下午 18:37 世界標
- 編輯時間：2022 年十一月十日，世界標準時間 18:37
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgeSchedulerReadOnlyAccess

說明： AmazonEventBridgeSchedulerReadOnlyAccess 受管理的政策會授與唯讀權限，以檢視排程和排程群組的詳細資料

AmazonEventBridgeSchedulerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEventBridgeSchedulerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二○二二年十一月十日，下午 18:50 世界標
- 編輯時間：2022 年十一月十日，世界標準時間 18:50
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgeSchemasFullAccess

描述：提供對 Amazon EventBridge 結構描述的完整存取權。

AmazonEventBridgeSchemasFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEventBridgeSchemasFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一九年十一月二十八日 23:12 世界標準
- 編輯時間：2019 年 11 月 28 日，世界標準時間 23:12
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgeSchemasReadOnlyAccess

說明：提供 Amazon EventBridge 結構描述的唯讀存取權限。

AmazonEventBridgeSchemasReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonEventBridgeSchemasReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一九年十一月二十八日 23:05 世界標準
- 編輯時間：2020 年 5 月 1 日，世界標準時間 00:50
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonEventBridgeSchemasServiceRolePolicy

說明：授與 Amazon EventBridge 結構描述建立的受管規則的許可。

`AmazonEventBridgeSchemasServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月二十七日, 01:10 世界標
- 編輯時間:2019 年十一月二十七日, 世界標準時間 1:10
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFISServiceRolePolicy

描述：啟用 AWS FIS 管理實驗監控和資源選擇的政策。

AmazonFISServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年十二月二十一日, 世界標準時間 21:18
- 編輯時間：2022 年 10 月 25 日（世界標準時間）09:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonForecastFullAccess

描述：可以訪問 Amazon Forecast 的所有操作

AmazonForecastFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonForecastFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 1 月 18 日, 01:52 世界標準時間
- 編輯時間:2019 年 1 月 18 日, 01:52 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonForecastFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFraudDetectorFullAccessPolicy

描述：可以訪問 Amazon Fraud Detector 的所有操作

`AmazonFraudDetectorFullAccessPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonFraudDetectorFullAccessPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 世界標準時間 22
- 編輯時間：2019 年 12 月 3 日，世界標準時間 22:46
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFreeRTOSFullAccess

說明：Amazon FreeRTOS 的完整存取政策

`AmazonFreeRTOSFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonFreeRTOSFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 11 月 29 日，世界標準時間下午 3:32
- 編輯時間：2017 年十一月二十九日，世界標準時間 15:32
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFreeRTOSOTAUpdate

說明：允許用戶訪問 Amazon FreeRTOS TA 更新

AmazonFreeRTOSOTAUpdate是AWS 受管理的策略。

使用此政策

您可以附加AmazonFreeRTOSOTAUpdate至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 8 月 27 日, 世界標準時間 22:43
- 編輯時間:2020 年十二月十八日, 世界標準時間 17:47
- ARN: arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFSxConsoleFullAccess

說明：提供對 Amazon FSx 的完整存取權，並 AWS 透過 AWS Management Console.

`AmazonFSxConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonFSxConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 11 月 28 日, 世界標準時間 16:36
- 編輯時間：世界標準時間 2024 年 1 月 10 日晚上 20:07
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFSxConsoleReadOnlyAccess

說明：提供 Amazon FSx 的唯讀存取權，以 AWS 及透過 AWS Management Console.

`AmazonFSxConsoleReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonFSxConsoleReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 11 月 28 日, 世界標準時間 16:35
- 編輯時間：世界標準時間 2024 年 1 月 10 日晚上 20:19
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFSxFullAccess

描述：提供對 Amazon FSx 的完整存取權限以及相關 AWS 服務的存取權。

AmazonFSxFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonFSxFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十八日, 16:34 世界標準時間
- 編輯時間：世界標準時間 2024 年 1 月 10 日晚上 20:16
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
```

```
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
```

```
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFSxReadOnlyAccess

說明：提供對 Amazon FSx 的唯讀存取權限。

AmazonFSxReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonFSxReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十八日, 世界標準時間 16:33
- 編輯時間：2018 年十一月二十八日，世界標準時間 16:33
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonFSxServiceRolePolicy

說明：允許 Amazon FSx 代表您管理 AWS 資源

AmazonFSxServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月二十八日, 世界標準時間 10:38
- 編輯時間：世界標準時間 2024 年 1 月 10 日晚上 20:53
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGlacierFullAccess

描述：提供完整的訪問 Amazon Glacier 通過 AWS Management Console.

AmazonGlacierFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonGlacierFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AmazonGlacierFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGlacierReadOnlyAccess

說明：提供透過 Amazon Glacier 的唯讀存取權限 AWS Management Console。

AmazonGlacierReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonGlacierReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2016 年 5 月 5 日，世界標準時間 18:46

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

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGrafanaAthenaAccess

說明：此政策授予對亞馬遜雅典娜的存取權，以及允許從 Amazon Grafana 中的 Amazon Athena 外掛程式向 s3 查詢和寫入結果所需的相依性。

AmazonGrafanaAthenaAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonGrafanaAthenaAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 2021 年十一月二十二日 17：11
- 編輯時間：2021 年十一月二十二日，世界標準時間 17:11
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGrafanaCloudWatchAccess

說明：此政策授予對 Amazon 的存取權限，以 CloudWatch 及在 Amazon 受管 Grafana 中用 CloudWatch 作資料來源所需的相依性。

AmazonGrafanaCloudWatchAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonGrafanaCloudWatchAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2023 年 3 月 24 日, 22:41

- **編輯時間**：世界標準時間 2023 年 3 月 24 日 22:41
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGrafanaRedshiftAccess

說明：此政策授予對 Amazon Redshift 的範圍存取權限，以及在 Amazon Grafana 中使用 Amazon Redshift 外掛程式所需的相依性。

AmazonGrafanaRedshiftAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonGrafanaRedshiftAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年十一月二十六日, 世界標準時間 23:15
- 編輯時間：2021 年十一月二十六日，世界標準時間 23:15
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGrafanaServiceLinkedRolePolicy

描述：提供對 Amazon Grafana 管理或使用的 AWS 資源的訪問。

AmazonGrafanaServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2022 年 11 月 8 日 23:10
- 編輯時間：2022 年 11 月 8 日，世界標準時間 23:10
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGuardDutyFullAccess

描述：提供使用 Amazon 的完全訪問權限 GuardDuty。

AmazonGuardDutyFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonGuardDutyFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月二十八日，世界標準時間 22:31
- 編輯時間：世界標準時間 2023 年 11 月 16 日 23:04
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGuardDutyMalwareProtectionServiceRolePolicy

說明： GuardDuty 惡意程式碼防護會使用名為的服務連結角色 (SLR)。AWSServiceRoleForAmazonGuardDutyMalwareProtection此服務連結角色可讓 GuardDuty

惡意程式碼防護執行無代理程式掃描，以偵測惡意程式碼。它 GuardDuty 允許在您的帳戶中創建快照，並與 GuardDuty 服務帳戶共享快照以掃描惡意軟件。它會評估這些共用快照，並將擷取的 EC2 執行個體中繼資料包含在 GuardDuty 惡意程式碼防護發現 AWSServiceRoleForAmazonGuardDutyMalwareProtection 服務連結的角色會信任惡意軟體保護。

AmazonGuardDutyMalwareProtectionServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 7 月 19 日，2022 年 7 月 19 日
- 編輯時間：世界標準時間 2024 年 1 月 25 日 22:24
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
```

```
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyScanId"
        }
      }
    },
    {
      "Sid" : "CreateTagsPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    },
    {
      "Sid" : "AddTagsToSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyExcluded",
            "GuardDutyFindingDetected"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteAndShareSnapshotPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "PreventPublicAccessToSnapshotPermission",
      "Effect" : "Deny",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/group" : "all"
        }
      }
    },
    {
      "Sid" : "CreateGrantPermission",
```

```
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "DescribeKeyPermission",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "GuardDutyLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid" : "GuardDutyLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
    {
      "Sid" : "EBSDirectAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGuardDutyReadOnlyAccess

說明：提供對 Amazon GuardDuty 資源的唯讀存取

AmazonGuardDutyReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonGuardDutyReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 11 月 28 日，世界標準時間 22:29
- 編輯時間：世界標準時間 2023 年 11 月 16 日 23:07
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonGuardDutyServiceRolePolicy

說明：啟用對 Amazon 警衛義務使用或管理的 AWS 資源的訪問

AmazonGuardDutyServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年十一月二十八日, 世界標準時間 20:12
- 編輯時間：世界標準時間 2024 年 3 月 27 日凌時 58 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHealthLakeFullAccess

描述：提供對 Amazon HealthLake 服務的完全訪問權限。

AmazonHealthLakeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonHealthLakeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 2 月 17 日, 世界標準時間 1:7
- 編輯時間:2021 年 2 月 17 日, 世界標準時間 1:07
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHealthLakeReadOnlyAccess

描述：提供對 Amazon HealthLake 服務的只讀訪問權限。

AmazonHealthLakeReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonHealthLakeReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 2 月 17 日, 02:43 世界標準時間
- 編輯時間:2021 年 2 月 17 日, 02:43 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHoneycodeFullAccess

描述：透過 AWS Management Console 和 SDK 提供對蜂 Honeycode 的完整存取權。

AmazonHoneycodeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonHoneycodeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 24 日, 世界標準時間 20:28
- 編輯時間：2020 年 6 月 24 日，世界標準時間 20:28
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHoneycodeReadOnlyAccess

說明：透過 AWS Management Console 和 SDK 提供蜂 Honeycode 的唯讀存取權。

AmazonHoneycodeReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonHoneycodeReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 24 日, 世界標準時間 20:28

- 編輯時間:2020 年十二月 1 日, 世界標準時間 17:27
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHoneycodeServiceRolePolicy

描述：Amazon 蜂 Honeycode 存取資源所需的服務連結角色。

AmazonHoneycodeServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年十一月十八日, 世界標準時間 18:03
- 編輯時間:2020 年十一月十八日, 世界標準時間 18:03
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHoneycodeTeamAssociationFullAccess

描述：透過 AWS Management Console 和 SDK 提供對蜂 Honeycode 團隊關聯的完整存取權。

AmazonHoneycodeTeamAssociationFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonHoneycodeTeamAssociationFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 24 日, 世界標準時間 20:28
- 編輯時間：2020 年 6 月 24 日，世界標準時間 20:28
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHoneycodeTeamAssociationReadOnlyAccess

描述：透過 AWS Management Console 和 SDK 提供蜂 Honeycode 團隊關聯的唯讀存取權。

AmazonHoneycodeTeamAssociationReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonHoneycodeTeamAssociationReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 24 日, 世界標準時間 20:27
- 編輯時間：2020 年 6 月 24 日，世界標準時間 20:27
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHoneycodeWorkbookFullAccess

描述：透過 AWS Management Console 和 SDK 提供對蜂 Honeycode 活頁簿的完整存取權。

AmazonHoneycodeWorkbookFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonHoneycodeWorkbookFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 24 日, 世界標準時間 20:28
- 編輯時間:2020 年十二月 1 日, 世界標準時間 17:30

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

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonHoneycodeWorkbookReadOnlyAccess

描述：透過 AWS Management Console 和 SDK 提供蜂 Honeycode 活頁簿的唯讀存取權。

AmazonHoneycodeWorkbookReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonHoneycodeWorkbookReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 24 日, 世界標準時間 20:28
- 編輯時間:2020 年十二月 1 日, 世界標準時間 17:32
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
```

```
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonInspector2AgentlessServiceRolePolicy

說明：授予 Amazon Inspector 執行無代理程式安全評估 AWS 服務 所需的存取權

`AmazonInspector2AgentlessServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 20 日，下午 3:18
- 編輯時間：世界標準時間 2023 年 11 月 20 日，下午 3:18
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonInspector2FullAccess

描述：提供對 Amazon Inspector 的完整存取權，以及其他相關服務 (例如組織) 的存取權。

AmazonInspector2FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonInspector2FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月二十九日，世界標準時間 19:10
- 編輯時間:世界標準時間 2024 年 4 月 25 日, 13:21
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonInspector2ManagedCisPolicy

描述：這是一個受管理的策略，客戶應該附加到他們的角色，以便與檢查員服務進行 CIS 掃描進行通信

AmazonInspector2ManagedCisPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonInspector2ManagedCisPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2024 年 1 月 24 日, 16:31
- 編輯時間:2024 年 1 月 24 日, 世界標準時間 16:31
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonInspector2ReadOnlyAccess

說明：提供 Amazon 檢查器 2 服務和相關支援服務的唯讀存取權

AmazonInspector2ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonInspector2ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 1 月 21 日，世界標準時間下午 2:45
- 編輯時間：世界標準時間 2023 年 9 月 22 日晚上 20:56
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonInspector2ServiceRolePolicy

說明：授予 Amazon Inspector 存取執行安全評估 AWS 服務 所需的權限

`AmazonInspector2ServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年十一月十六日, 世界標準時間 20:27
- 編輯時間：世界標準時間 2024 年 1 月 22 日下午 2:06
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

政策版本

策略版本：v12(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonInspectorFullAccess

描述：提供對 Amazon Inspector 的完全訪問。

AmazonInspectorFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonInspectorFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**二零一五年十月七日, 17:08 世界標準時間
- **編輯時間**：2017 年十二月二十一日，世界標準時間 14:53
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonInspectorReadOnlyAccess

描述：提供對 Amazon Inspector 的只讀訪問權限。

AmazonInspectorReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonInspectorReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一五年十月七日, 17:08 世界標準時間
- 編輯時間:二零一九年十月一日, 世界標準時間 15:17
- ARN: arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonInspectorServiceRolePolicy

說明：授予 Amazon Inspector 存取執行安全評估 AWS 服務 所需的權限

AmazonInspectorServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年 11 月 21 日，世界標準時間 15:48
- 編輯時間：2020 年 9 月 11 日，世界標準時間 17：12
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKendraFullAccess

說明:提供完整的存取權限 Amazon Kendra 透過 AWS Management Console.

AmazonKendraFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonKendraFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 16:15 世界標準時
- 編輯時間：2019 年 12 月 3 日，世界標準時間 16:15
- ARN: arn:aws:iam::aws:policy/AmazonKendraFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKendraReadOnlyAccess

說明：透過提供 Amazon Kendra 的 AWS Management Console唯讀存取權限。

AmazonKendraReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonKendraReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 16:13 世界標準時

- 編輯時間:2021 年 5 月 27 日, 世界標準時間 17:01
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKeyspacesFullAccess

描述：提供對 Amazon Keyspaces 的完全訪問

AmazonKeyspacesFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonKeyspacesFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 23 日, 世界標準時間 17:06
- 編輯時間：世界標準時間 2023 年 10 月 3 日晚上 19 時 12 分
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKeyspacesReadOnlyAccess

說明：提供對 Amazon Keyspaces 的只讀訪問權限

AmazonKeyspacesReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonKeyspacesReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 23 日, 世界標準時間 17:07
- 編輯時間：2022 年 7 月 7 日，世界標準時間 14:54
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKeyspacesReadOnlyAccess_v2

說明：提供 Amazon Keyspaces 和相關 AWS 服務的唯讀存取權限。

AmazonKeyspacesReadOnlyAccess_v2是AWS 受管理的策略。

使用此政策

您可以附加AmazonKeyspacesReadOnlyAccess_v2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 9 月 12 日, 17:01
- 編輯時間：世界標準時間 2023 年 9 月 12 日下午 17 時 01 分
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKinesisAnalyticsFullAccess

說明：提供完整的 Amazon Kinesis Analytics，透過 AWS Management Console.

`AmazonKinesisAnalyticsFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonKinesisAnalyticsFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2016 年 9 月 21 日，世界標準時間 19:01
- 編輯時間：2016 年 9 月 21 日，世界標準時間 19:01
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKinesisAnalyticsReadOnly

說明：透過提供 Amazon Kinesis Analytics 的 AWS Management Console唯讀存取權。

AmazonKinesisAnalyticsReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonKinesisAnalyticsReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2016 年 9 月 21 日, 世界標準時間 18:16
- 編輯時間：2016 年 9 月 21 日，世界標準時間 18:16
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKinesisFirehoseFullAccess

描述：提供對所有 Amazon Kinesis Firehose 交付串流的完整存取權。

AmazonKinesisFirehoseFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonKinesisFirehoseFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:十月七日, 2015, 18:45 世界標準時間
- 編輯時間:2015 年 10 月 7 日, 世界標準時間 18:45
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKinesisFirehoseReadOnlyAccess

描述：提供對所有 Amazon Kinesis Firehose 交付串流的唯讀存取權。

`AmazonKinesisFirehoseReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonKinesisFirehoseReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一五年十月七日, 18:43 世界標準時間
- 編輯時間:十月七日, 2015, 18:43 世界標準時間
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKinesisFullAccess

說明：透過提供對所有串流的完整存取 AWS Management Console。

AmazonKinesisFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonKinesisFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40

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

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKinesisReadOnlyAccess

說明：透過提供所有串流的唯讀存取權 AWS Management Console。

`AmazonKinesisReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonKinesisReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKinesisVideoStreamsFullAccess

說明：可透過以下 AWS Management Console方式提供 Amazon Kinesis Video Streams 的完整存取權。

AmazonKinesisVideoStreamsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonKinesisVideoStreamsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 12 月 1 日, 23:27 世界標準時間
- 編輯時間：2017 年 12 月 1 日，世界標準時間 23:27
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonKinesisVideoStreamsReadOnlyAccess

說明：透過提供 AWS Kinesis Video Streams 的 AWS Management Console唯讀存取權。

`AmazonKinesisVideoStreamsReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonKinesisVideoStreamsReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一七年十二月一日 23:14 世界標準時間
- 編輯時間：2017 年 12 月 1 日，世界標準時間 23:14
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLaunchWizard_Fullaccess

描述： AWS 啟動精靈和其他必要服務的完整存取權。

AmazonLaunchWizard_Fullaccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonLaunchWizard_Fullaccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 6 日, 世界標準時間 17:47
- 編輯時間：世界標準時間 2023 年 2 月 22 日 17:25
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess

政策版本

策略版本：v15(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLaunchWizardFullAccessV2

描述： AWS 啟動精靈和其他必要服務的完整存取權。

AmazonLaunchWizardFullAccessV2是AWS 受管理的策略。

使用此政策

您可以附加AmazonLaunchWizardFullAccessV2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 9 月 1 日, 17:14
- 編輯時間：世界標準時間 2023 年 9 月 1 日下午 17 時 14 分
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLexChannelsAccess

說明：此原則可讓客戶從通道呼叫 Lex 執行階段

AmazonLexChannelsAccess是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- 創建時間:2021 年 1 月 13 日, 世界標準時間 20:12
- 編輯時間:2021 年 1 月 13 日, 世界標準時間 20:12
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLexFullAccess

說明：提供完整的存取權限 Amazon Lex 透過 AWS Management Console. 此外，還提供建立 Lex 服務連結角色的存取權，並授與 Lex 權限，以叫用有限的 Lambda 函數集。

`AmazonLexFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加AmazonLexFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 4 月 11 日, 23:20 世界標準時間
- 編輯時間:世界標準時間 2024 年 4 月 16 日, 20:06
- ARN: arn:aws:iam::aws:policy/AmazonLexFullAccess

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLexReadOnly

說明：提供 Amazon Lex 的唯讀存取權限。

AmazonLexReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonLexReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 4 月 11 日, 23:13 世界標準時間
- 編輯時間：2024 年 5 月 13 日，世界標準時間 16:58
- ARN: arn:aws:iam::aws:policy/AmazonLexReadOnly

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLexReplicationPolicy

說明：允許 Amazon Lex 代表您跨區域複寫 Lex 資源。

AmazonLexReplicationPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2024 年 1 月 31 日 23:29
- 編輯時間：世界標準時間 2024 年 3 月 8 日下午 17 時 11 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLexRunBotsOnly

說明：提供對 Amazon Lex 交談式 API 的存取權。

AmazonLexRunBotsOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonLexRunBotsOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 4 月 11 日, 世界標準時間 23:06
- 編輯時間：2021 年 8 月 18 日，世界標準時間 00:15
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLexV2BotPolicy

描述：提供 Lex V2 機器人存取權，以代表您呼叫其他 AWS 服務。

AmazonLexV2BotPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 1 月 13 日, 世界標準時間 20:10
- 編輯時間:2021 年 1 月 13 日, 世界標準時間 20:10
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLookoutEquipmentFullAccess

說明：提供對 Amazon 瞭望設備操作的完整訪問權限

AmazonLookoutEquipmentFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonLookoutEquipmentFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 4 月 8 日, 下午 3:52 世界標準時間
- 編輯時間：2021 年 11 月 24 日，世界標準時間 21 點 00
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLookoutEquipmentReadOnlyAccess

說明：提供對 Amazon 觀景設備的只讀訪問

AmazonLookoutEquipmentReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonLookoutEquipmentReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 5 月 5 日, 16:47 世界標準時間
- 編輯時間：二○二二年十一月十日，世界標準時間 22
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLookoutMetricsFullAccess

描述：可以訪問 Amazon Lookout for Metrics 的所有操作

`AmazonLookoutMetricsFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonLookoutMetricsFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 5 月 7 日，世界標準時間 00:43
- 編輯時間：2021 年 5 月 7 日，世界標準時間 00:43
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLookoutMetricsReadOnlyAccess

說明：授予 Amazon 瞭望指標的所有唯讀動作存取權

AmazonLookoutMetricsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonLookoutMetricsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 5 月 7 日，世界標準時間 00:43
- 編輯時間：世界標準時間 2022 年 1 月 4 日 18:19
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLookoutVisionConsoleFullAccess

描述：提供對於視覺的 Amazon Lookout 的完整存取權，以及所需服務和主控台相依性的範圍存取權限。

AmazonLookoutVisionConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonLookoutVisionConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 5 月 11 日, 世界標準時間 19:37
- 編輯時間：2021 年 5 月 11 日，世界標準時間 19:37
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLookoutVisionConsoleReadOnlyAccess

描述：提供 Amazon Lookout for Vision 的唯讀存取權限，以及所需服務和主控台相依性的範圍存取權。

AmazonLookoutVisionConsoleReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonLookoutVisionConsoleReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 5 月 11 日, 世界標準時間 19:32
- 編輯時間：世界標準時間十二月九日，2021 年 02 月 46 日
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLookoutVisionFullAccess

描述：提供對 Amazon Lookout 視覺的完整存取權，以及所需相依性的範圍存取權限。

AmazonLookoutVisionFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonLookoutVisionFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 5 月 11 日, 世界標準時間 19:24
- 編輯時間：2021 年 5 月 11 日，世界標準時間 19:24
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonLookoutVisionReadOnlyAccess

說明：提供 Amazon Lookout for Vision 的唯讀存取權限，以及所需相依性的範圍存取權限。

`AmazonLookoutVisionReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonLookoutVisionReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**:2021 年 5 月 11 日, 世界標準時間 19:11
- **編輯時間**：2021 年十二月九日，03:01 世界標準時間
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMachineLearningBatchPredictionsAccess

說明：授予使用者請求 Amazon Machine Learning 批次預測的權限。

AmazonMachineLearningBatchPredictionsAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMachineLearningBatchPredictionsAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 4 月 9 日, 17:12 世界標準時間
- 編輯時間:2015 年 4 月 9 日, 17:12 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMachineLearningCreateOnlyAccess

說明：提供非預測 Amazon Machine Learning 資源的建立存取權。

AmazonMachineLearningCreateOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMachineLearningCreateOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 4 月 9 日, 17:18 世界標準時間
- 編輯時間：2016 年 6 月 29 日，世界標準時間 20:55
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMachineLearningFullAccess

描述：提供對 Amazon Machine Learning 資源的完整存取權。

AmazonMachineLearningFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMachineLearningFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- 創建時間:2015 年 4 月 9 日, 17:25 世界標準時間
- 編輯時間:2015 年 4 月 9 日, 17:25 世界標準時間
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

說明：授予使用者建立和刪除 Amazon Machine Learning 模型即時端點的權限。

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加AmazonMachineLearningManageRealTimeEndpointOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 4 月 9 日, 17:32 世界標準時間
- 編輯時間:2015 年 4 月 9 日, 17:32 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMachineLearningReadOnlyAccess

說明：提供 Amazon Machine Learning 資源的唯讀存取權。

AmazonMachineLearningReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMachineLearningReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 4 月 9 日, 17:40 世界標準時間
- 編輯時間:2015 年 4 月 9 日, 17:40 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMachineLearningRealTimePredictionOnlyAccess

說明：授予使用者請求 Amazon Machine Learning 即時預測的權限。

AmazonMachineLearningRealTimePredictionOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMachineLearningRealTimePredictionOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 4 月 9 日, 17:44 世界標準時間
- 編輯時間:2015 年 4 月 9 日, 17:44 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMachineLearningRoleforRedshiftDataSourceV3

描述：允許 Machine Learning 針對 Redshift 資料來源設定和使用 Redshift 叢集和 S3 暫存位置。

AmazonMachineLearningRoleforRedshiftDataSourceV3是AWS 受管理的策略。

使用此政策

您可以附加AmazonMachineLearningRoleforRedshiftDataSourceV3至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2020 年 6 月 24 日，世界標準時間 18:00
- 編輯時間：2020 年 6 月 24 日（世界標準時間）18:00

- ARN: arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMacieFullAccess

描述：提供對 Amazon Macie 的完全訪問權限。

AmazonMacieFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMacieFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 8 月 14 日，世界標準時間 14:54
- 編輯時間：世界標準時間：2022 年 7 月 1 日凌晨 4 時 41
- ARN: arn:aws:iam::aws:policy/AmazonMacieFullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMacieHandshakeRole

說明：授予建立 Amazon Macie 服務連結角色的權限。

AmazonMacieHandshakeRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonMacieHandshakeRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 6 月 28 日, 世界標準時間 15:46
- 編輯時間:2018 年 6 月 28 日, 世界標準時間 15:46
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMacieReadOnlyAccess

描述：提供對 Amazon Macie 的只讀訪問權限。

AmazonMacieReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMacieReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 6 月 15 日, 21:50
- 編輯時間：世界標準時間 2023 年 6 月 15 日晚上 9 時 50 分
- ARN: arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
```

```
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMacieServiceRole

說明：授予 Macie 對帳戶中資源相依性的唯讀存取權限，以便啟用資料分析。

AmazonMacieServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonMacieServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2017 年 8 月 14 日，世界標準時間 14:53
- 編輯時間：2017 年 8 月 14 日，世界標準時間 14:53
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMacieServiceRolePolicy

說明：Amazon Macie 的服務連結角色

AmazonMacieServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 6 月 19 日, 世界標準時間 22:17
- 編輯時間：2022 年 5 月 19 日，世界標準時間 19:16

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

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonManagedBlockchainConsoleFullAccess

說明：提供 Amazon Managed Blockchain 的完整存取權 AWS Management Console

`AmazonManagedBlockchainConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonManagedBlockchainConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**2019 年 4 月 29 日, 世界標準時間 21:23
- **編輯時間:**2019 年 4 月 29 日, 世界標準時間 21:23
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonManagedBlockchainFullAccess

描述：提供對 Amazon Managed Blockchain 的完整存取權。

AmazonManagedBlockchainFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonManagedBlockchainFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 4 月 29 日, 21:39 世界標準時間
- 編輯時間:2019 年 4 月 29 日, 世界標準時間 21:39
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonManagedBlockchainReadOnlyAccess

說明：提供 Amazon Managed Blockchain 的唯讀存取權。

`AmazonManagedBlockchainReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonManagedBlockchainReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 4 月 30 日, 世界標準時間 18:17
- 編輯時間:2019 年 4 月 30 日, 世界標準時間 18:17
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:Get*",
        "managedblockchain:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonManagedBlockchainServiceRolePolicy

說明：允許存取 Amazon AWS 服務 受管區塊鏈所使用或管理的資源

AmazonManagedBlockchainServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 1 月 17 日, 世界標準時間 19:51
- 編輯時間:2020 年 1 月 17 日, 世界標準時間 19:51
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMCSFullAccess

描述：提供完全訪問 Amazon 託管的 Apache 卡桑德拉服務

AmazonMCSFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMCSFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 13:45 世界標準時
- 編輯時間:2020 年 4 月 17 日, 世界標準時間 19:19
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMCSReadOnlyAccess

描述：提供 Amazon 託管 Apache 卡桑德拉服務的只讀訪問

AmazonMCSReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMCSReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 13:46 世界標準時
- 編輯時間:2020 年 4 月 17 日, 世界標準時間 19:21
- ARN: arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMechanicalTurkFullAccess

描述：提供對 Amazon Mechanical Turk 中所有 API 的完整訪問權限。

AmazonMechanicalTurkFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMechanicalTurkFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：十二月十一日，二零一五年十二月十一日
- 編輯時間：2015 年十二月十一日，世界標準時間 19:08
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMechanicalTurkReadOnly

描述：提供 Amazon Mechanical Turk 中唯讀 API 的訪問權限。

AmazonMechanicalTurkReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonMechanicalTurkReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：十二月十一日，二零一五年十二月十一日

- 編輯時間：2019 年 9 月 25 日，世界標準時間 21:06
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMemoryDBFullAccess

說明：提供完整的存取 Amazon 記憶體資料庫，透過. AWS Management Console

AmazonMemoryDBFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMemoryDBFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二一年十月八日, 19:24 世界標準時間
- 編輯時間：2021 年 10 月 8 日，世界標準時間 19:24
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMemoryDBReadOnlyAccess

說明：透過提供 Amazon 記憶體的唯讀存取權限。 AWS Management Console

AmazonMemoryDBReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMemoryDBReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二一年十月八日, 19:27 世界標準時間
- 編輯時間：2021 年 10 月 8 日，世界標準時間 19:27
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMobileAnalyticsFinancialReportAccess

描述：提供所有報表的唯讀存取權，包括所有應用程式資源的財務資料。

AmazonMobileAnalyticsFinancialReportAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMobileAnalyticsFinancialReportAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40

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

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMobileAnalyticsFullAccess

描述：提供對所有應用程式資源的完整存取權。

`AmazonMobileAnalyticsFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加AmazonMobileAnalyticsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMobileAnalyticsNon-financialReportAccess

摘要：針對所有應用程式資源，提供非財務報表的唯讀存取權。

AmazonMobileAnalyticsNon-financialReportAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMobileAnalyticsNon-financialReportAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMobileAnalyticsWriteOnlyAccess

描述：提供對所有應用程式資源置入事件資料的僅寫入存取權。(建議用於 SDK 整合)

AmazonMobileAnalyticsWriteOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMobileAnalyticsWriteOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:PutEvents",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMonitronFullAccess

說明：提供管理 Amazon Monitron 的完整存取權

AmazonMonitronFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMonitronFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 12 月 2 日, 世界標準時間 22:40
- 編輯時間：2022 年 6 月 8 日，世界標準時間 16:27
- ARN: arn:aws:iam::aws:policy/AmazonMonitronFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMQApiFullAccess

說明：透過我們的 API/SDK 提供對 AmazonMQ 的完整存取權。

AmazonMQApiFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMQApiFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十二月十八日, 世界標準時間 20:31
- 編輯時間：2020 年 11 月 4 日，世界標準時間 16:45
- ARN: arn:aws:iam::aws:policy/AmazonMQApiFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMQApiReadOnlyAccess

說明：透過我們的 API/SDK 提供對 AmazonMQ 的唯讀存取權限。

AmazonMQApiReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMQApiReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十二月十八日, 世界標準時間 20:31
- 編輯時間：2018 年十二月十八日，世界標準時間 20:31
- ARN: arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMQFullAccess

說明：提供透過. AWS Management Console

AmazonMQFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMQFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 11 月 28 日，世界標準時間 15:28
- 編輯時間：2020 年 11 月 4 日，世界標準時間 16:34
- ARN: arn:aws:iam::aws:policy/AmazonMQFullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMQReadOnlyAccess

說明 AmazonMQ 透過. AWS Management Console

`AmazonMQReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonMQReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 11 月 28 日, 世界標準時間下午 3 點 30
- 編輯時間：2017 年十一月二十八日，世界標準時間 19:02
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMQServiceRolePolicy

說明：適用於 AWS Amazon MQ 的服務連結角色政策

AmazonMQServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間**:2020 年 11 月 4 日, 世界標準時間 16:07
- **編輯時間**：2020 年 11 月 4 日，世界標準時間 16:07
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMSKConnectReadOnlyAccess

說明：提供對 Amazon MSK Connect 的只讀訪問

AmazonMSKConnectReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMSKConnectReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 9 月 20 日, 世界標準時間 10:18
- 編輯時間:2021 年 10 月 18 日, 09:16 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMSKFullAccess

說明：提供 Amazon MSK 的完整存取權限，以及其相依性的其他必要許可。

AmazonMSKFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMSKFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2019 年 1 月 14 日, 世界標準時間 22:07
- 編輯時間：世界標準時間 2023 年 10 月 18 日 11:33
- ARN: arn:aws:iam::aws:policy/AmazonMSKFullAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMSKReadOnlyAccess

說明：提供對 Amazon MSK 的只讀訪問

AmazonMSKReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonMSKReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**：2019 年 1 月 14 日, 世界標準時間 22:28
- **編輯時間**：2019 年 1 月 14 日, 世界標準時間 22:28
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonMWAAServiceRolePolicy

說明：用於 Apache 氣流的 Amazon 受管工作流程所使用的服務連結角色。

AmazonMWAAServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2020 年十一月二十四日，世界標準時間 14:13
- 編輯時間：2022 年十一月十七日，世界標準時間 00:56
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonNimbleStudio-LaunchProfileWorker

說明：此政策授予對敏捷工作室啟動設定檔工作者所需資源的存取權。將此政策附加到靈活工作室生成器創建的 EC2 實例。

AmazonNimbleStudio-LaunchProfileWorker是AWS 受管理的策略。

使用此政策

您可以附加AmazonNimbleStudio-LaunchProfileWorker至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 4 月 28 日, 04:47 世界標準時間
- 編輯時間:2021 年 4 月 28 日, 04:47 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonNimbleStudio-StudioAdmin

說明：此政策授予與工作室管理員和其他服務中相關工作室資源相關聯的 Amazon Nimble Studio 資源的存取權。將此原則附加到與您的工作室相關聯的管理員角色。

AmazonNimbleStudio-StudioAdmin是AWS 受管理的策略。

使用此政策

您可以附加AmazonNimbleStudio-StudioAdmin至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 4 月 28 日, 04:47 世界標準時間
- 編輯時間：世界標準時間 2023 年 9 月 22 日下午 17 時 40 分
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonNimbleStudio-StudioUser

說明：此政策授予存取與工作室使用者相關聯的 Amazon Nimble Studio 資源，以及其他服務中的相關工作室資源。將此原則附加到與您的工作室相關聯的使用者角色。

AmazonNimbleStudio-StudioUser是AWS 受管理的策略。

使用此政策

您可以附加AmazonNimbleStudio-StudioUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 4 月 28 日, 04:48 世界標準時間
- 編輯時間：世界標準時間 2023 年 9 月 22 日下午 17 時 45 分
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOmicsFullAccess

描述：提供對 Amazon Oomics 和其他必要項 AWS 服務目的完整存取權。此原則可讓使用者檢視及接受 RAM 共用邀請，以存取使用者以外的資源 AWS 帳戶。

AmazonOmicsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOmicsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2023 年 2 月 24 日，00:59 世界標準時間
- 編輯時間：世界標準時間 2023 年 2 月 24 日凌時 59 分
- ARN: arn:aws:iam::aws:policy/AmazonOmicsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOmicsReadOnlyAccess

說明：提供 Amazon 組合的唯讀存取權

AmazonOmicsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOmicsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間（世界標準時間）11 月 29 日
- 編輯時間：世界標準時間十一月二十九日（二零二）
- ARN: arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOneEnterpriseFullAccess

說明：此政策授予允許存取所有 Amazon One 企業資源和操作的管理許可。

AmazonOneEnterpriseFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOneEnterpriseFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 11 月 28 日, 04:58 世界標準時間
- 編輯時間:2023 年 11 月 28 日, 04:58 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOneEnterpriseInstallerAccess

說明：此原則授予有限的讀取和寫入權限，允許裝置安裝和啟用。

AmazonOneEnterpriseInstallerAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOneEnterpriseInstallerAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 11 月 28 日凌晨 5 點
- 編輯時間：世界標準時間 2023 年 11 月 28 日凌晨 5 點
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOneEnterpriseReadOnlyAccess

說明：此政策授予所有 Amazon One 企業資源和操作的唯讀權限。

AmazonOneEnterpriseReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOneEnterpriseReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 11 月 28 日, 04:59 世界標準時間

- 編輯時間:2023 年 11 月 28 日, 04:59 世界標準時間
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchDashboardsServiceRolePolicy

說明：提供 Amazon OpenSearch 儀表板服務的存取權，以存取其他 AWS 服務，例如 CloudWatch 代表您

AmazonOpenSearchDashboardsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 12 月 22 日，下午 19:38
- 編輯時間：世界標準時間 2023 年十二月二十二日下午 19:38
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchDirectQueryGlueCreateAccess

描述：允許 OpenSearch DirectQuery 服務存取 AWS Glue API，以代表您建立資源。

AmazonOpenSearchDirectQueryGlueCreateAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOpenSearchDirectQueryGlueCreateAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 5 月 6 日，下午 12:24
- 編輯時間：世界標準時間 5 月 6 日，下午 12:24
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchIngestionFullAccess

描述：允許 Amazon OpenSearch 擷取代您存取其他 AWS 服務。

AmazonOpenSearchIngestionFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOpenSearchIngestionFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 26 日, 世界標準時間 18:11
- 編輯時間：世界標準時間 2023 年 4 月 26 日下午 18:11
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchIngestionReadOnlyAccess

說明：提供 Amazon OpenSearch 擷取服務的唯讀存取權

AmazonOpenSearchIngestionReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOpenSearchIngestionReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 26 日, 世界標準時間 18:09
- 編輯時間:世界標準時間 2023 年 4 月 26 日, 18:09
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchIngestionServiceRolePolicy

描述：允許 Amazon OpenSearch 擷取服務代表您存取其他 AWS 服務。

`AmazonOpenSearchIngestionServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：2022 年十一月十八日，16:49
- 編輯時間：2022 年十一月十八日，世界標準時間 16:49
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchServerlessServiceRolePolicy

說明：允許 Amazon OpenSearch 無伺服器代表您存取其他 AWS 服務，例如 CloudWatch API。

`AmazonOpenSearchServerlessServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2022 年十一月二十四日，世界標準時間 19:50
- 編輯時間：2022 年十一月二十四日，世界標準時間 19:50
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSS"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchServiceCognitoAccess

描述：提供對 Amazon Cognito 組態服務的存取權。

AmazonOpenSearchServiceCognitoAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOpenSearchServiceCognitoAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 9 月 2 日, 06:31 世界標準時間
- 編輯時間：2021 年十二月二十日，世界標準時間 14:04
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchServiceFullAccess

描述：提供對 Amazon OpenSearch 服務組態服務的完整存取權。

AmazonOpenSearchServiceFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOpenSearchServiceFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 9 月 8 日，5：33
- 編輯時間:2021 年 9 月 8 日, 12:33 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchServiceReadOnlyAccess

描述：提供 Amazon OpenSearch 服務組態服務的唯讀存取權。

AmazonOpenSearchServiceReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonOpenSearchServiceReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 9 月 8 日，世界標準時間 12:38
- 編輯時間：2021 年 9 月 8 日，世界標準時間 5：38
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonOpenSearchServiceRolePolicy

說明：允許 Amazon OpenSearch 服務代表您訪問其他 AWS 服務，例如 EC2 聯網 API。

AmazonOpenSearchServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間**:2021 年 8 月 26 日, 09:27 世界標準時間
- **編輯時間**:世界標準時間 2023 年 10 月 23 日, 07:07
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonPersonalizeFullAccess

描述：提供透過 AWS Management Console 和 SDK 對 Amazon Personalize 的完整存取權。也提供對相關服務 (例如 S3、 CloudWatch) 的選取存取權限。

AmazonPersonalizeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonPersonalizeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 12 月 4 日, 世界標準時間 22:24
- 編輯時間：2019 年 5 月 30 日，世界標準時間 23:46
- ARN: arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonPollyFullAccess

說明：授予對 Amazon Polly 服務和資源的完整存取權限。

AmazonPollyFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonPollyFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：十一月三十日，二零一六年十一月三十日
- 編輯時間：2016 年 11 月 30 日，世界標準時間 18:59
- ARN: arn:aws:iam::aws:policy/AmazonPollyFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonPollyReadOnlyAccess

說明：授予對 Amazon Polly 資源的唯讀存取權。

AmazonPollyReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonPollyReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：十一月三十日，二零一六年十一月三十日
- 編輯時間:2018 年 7 月 17 日, 世界標準時間 16:41
- ARN: arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonPrometheusConsoleFullAccess

描述：授與主控台中 AWS 受管理的 Prometheus 資源的完整存取權 AWS

`AmazonPrometheusConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonPrometheusConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十五日, 世界標準時間 18:11
- 編輯時間：2022 年 10 月 24 日，世界標準時間 22:25
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonPrometheusFullAccess

描述：授予 AWS 受管理的 Prometheus 資源的完整存取權

AmazonPrometheusFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonPrometheusFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十五日, 世界標準時間 18:10
- 編輯時間：世界標準時間：2023 年 11 月 26 日，晚上 20:16
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonPrometheusQueryAccess

描述：授與對 AWS 受管理的 Prometheus 資源執行查詢的存取權

AmazonPrometheusQueryAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonPrometheusQueryAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十九日, 01:02 世界標準時間
- 編輯時間:2020 年十二月十九日, 01:02 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonPrometheusRemoteWriteAccess

描述：授與 AWS 受管理的 Prometheus 工作區的唯寫存取權

AmazonPrometheusRemoteWriteAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonPrometheusRemoteWriteAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十九日, 01:04 世界標準時間
- 編輯時間:2020 年十二月十九日, 01:04 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonPrometheusScraperServiceRolePolicy

說明：提供存取由 Amazon 管 AWS 理服務為 Prometheus 收集器管理或使用的資源

AmazonPrometheusScraperServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 26 日，下午 4 時 19 分
- 編輯時間:2020 年 4 月 26 日, 世界標準時間 20:25
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "ENIUpdating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "EKSAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
```

```
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DeleteEKSAccessEntry",
      "Effect" : "Allow",
      "Action" : "eks:DeleteAccessEntry",
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
        }
      }
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonQFullAccess

說明：提供完整存取權以啟用與 Amazon Q 互動

AmazonQFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonQFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 11 月 28 日下午 4 點
- 編輯時間：世界標準時間 2024 年 4 月 29 日 17:02
- ARN: arn:aws:iam::aws:policy/AmazonQFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonQLDBConsoleFullAccess

說明：提供完整的 Amazon QLDB 存取權，透過. AWS Management Console

`AmazonQLDBConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonQLDBConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 9 月 5 日, 世界標準時間 18:24
- 編輯時間：2022 年 11 月 4 日，世界標準時間下午 17 時 01
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonQLDBFullAccess

說明：透過服務 API 提供對 Amazon QLDB 的完整存取權。

AmazonQLDBFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonQLDBFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 9 月 5 日, 世界標準時間 18:23
- 編輯時間：2022 年 11 月 4 日，世界標準時間下午 17 時 01
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonQLDBReadOnly

說明：提供對 Amazon QLDB 的唯讀存取。

AmazonQLDBReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonQLDBReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 9 月 5 日, 世界標準時間 18:19
- 編輯時間:世界標準時間 7 月 2 日, 下午 2 時 17 分
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSBetaServiceRolePolicy

描述：允許 Amazon RDS 代表您管理 AWS 資源。

AmazonRDSBetaServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 5 月 2 日, 世界標準時間 19:41
- 編輯時間：2022 年十二月十四日，世界標準時間 18:33
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSCustomInstanceProfileRolePolicy

說明：允許 Amazon RDS 自訂透過 EC2 執行個體設定檔執行各種自動化動作和資料庫管理任務。

AmazonRDSCustomInstanceProfileRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonRDSCustomInstanceProfileRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間:2024 年 2 月 27 日, 17:42
- 編輯時間：世界標準時間 2024 年 2 月 27 日 17:42
- ARN: arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSCustomPreviewServiceRolePolicy

說明：Amazon RDS 自訂預覽服務角色政策

AmazonRDSCustomPreviewServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零二一年十月八日, 21:44 世界標準時間
- 編輯時間：世界標準時間 2023 年 9 月 20 日下午 17 時 48 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSCustomServiceRolePolicy

說明：允許 Amazon RDS 自訂代表您管理 AWS 資源。

AmazonRDSCustomServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零二一年十月八日, 21:39 世界標準時間
- 編輯時間:世界標準時間 2024 年 4 月 19 日, 15:15
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSDataFullAccess

描述：允許完整存取使用 RDS 資料 API、RDS 資料庫認證的秘密存放區 API，以及資料庫主控台查詢管理 API，以便在中的 Aurora 無伺服器叢集上執行 SQL 陳述式。 AWS 帳戶

AmazonRDSDataFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRDSDataFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一八年十一月二十日, 21:29 世界時間
- 編輯時間：2019 年 11 月 20 日，世界標準時間 21:58
- ARN: arn:aws:iam::aws:policy/AmazonRDSDataFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSDirectoryServiceAccess

說明：允許 RDS 代表客戶針對加入網域的 SQL Server 資料庫執行個體存取 Directory Service 受管理的 AD。

AmazonRDSDirectoryServiceAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRDSDirectoryServiceAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一六年二月二十六日, 02:02 世界時間
- 編輯時間：2019 年 5 月 15 日，世界標準時間 16:51
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSEnhancedMonitoringRole

說明：提供 RDS 增強型監控的雲觀察存取權

AmazonRDSEnhancedMonitoringRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonRDSEnhancedMonitoringRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：十一月十一日，二零一五年十一月十一日
- 編輯時間：2015 年 11 月 11 日，世界標準時間 19:58
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSFullAccess

說明：提 Amazon 透過 AWS Management Console.

AmazonRDSFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRDSFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2023 年 8 月 17 日晚上 11 點
- ARN: arn:aws:iam::aws:policy/AmazonRDSFullAccess

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSPerformanceInsightsFullAccess

說明：提供 RDS Performance Insights 的完整存取權，透過 AWS Management Console

`AmazonRDSPerformanceInsightsFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonRDSPerformanceInsightsFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 8 月 15 日 23:41
- 編輯時間：世界標準時間 2023 年 10 月 23 日晚上 14 分
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSPerformanceInsightsReadOnly

說明：RDS Performance Insights 的唯讀原則

AmazonRDSPerformanceInsightsReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonRDSPerformanceInsightsReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 4 月 5 日，世界標準時間 00:02
- 編輯時間：世界標準時間 2023 年 10 月 23 日晚上 9 時 17 分
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSPreviewServiceRolePolicy

說明：Amazon RDS 預覽服務角色政策

AmazonRDSPreviewServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 5 月 31 日, 世界標準時間 18:02
- 編輯時間：世界標準時間 2023 年 10 月 4 日晚上 19 時 01 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSReadOnlyAccess

說明：透過提供 Amazon RDS 的唯讀存取權 AWS Management Console。

AmazonRDSReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRDSReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2023 年 4 月 14 日 12:32
- ARN: arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRDSServiceRolePolicy

描述：允許 Amazon RDS 代表您管理 AWS 資源。

AmazonRDSServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 1 月 8 日, 18:17 世界標準時間
- 編輯時間：世界標準時間 2024 年 1 月 19 日下午 3:10
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy

政策版本

策略版本：v13(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftAllCommandsFullAccess

說明：此政策包括執行 SQL 命令的許可，以便在 Amazon Redshift 上複製、載入、卸載、查詢和分析資料。該政策還授予許可，以執行相關服務 (例如 Amazon S3、Amazon CloudWatch 日誌、Amazon SageMaker 或 AWS Glue) 的選取陳述式。

`AmazonRedshiftAllCommandsFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加AmazonRedshiftAllCommandsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 11 月 4 日，世界標準時間 00:48
- 編輯時間:2021 年十一月 25 日, 02:27 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftDataFullAccess

說明：此政策提供對 Amazon Redshift 資料 API 的完整存取權。此政策也會授予範圍存取其他必要服務的權限。

AmazonRedshiftDataFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRedshiftDataFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 9 月 9 日，世界標準時間 19:23
- 編輯時間:世界標準時間 2023 年 4 月 7 日, 18:18
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftFullAccess

說明：提供完整的 Amazon Redshift 取權限，透過 AWS Management Console.

AmazonRedshiftFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRedshiftFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間

- 編輯時間：2022 年 7 月 7 日，世界標準時間 23:31
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftFullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftQueryEditor

說明：提供對 Amazon Redshift 查詢編輯器的完整存取權，以及透過 AWS Management Console.

AmazonRedshiftQueryEditor是AWS 受管理的策略。

使用此政策

您可以附加AmazonRedshiftQueryEditor至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 4 日, 世界標準時間 22:50
- 編輯時間：2021 年 2 月 16 日，世界標準時間 19:33
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftQueryEditorV2FullAccess

說明：授予對 Amazon Redshift 查詢編輯器 V2 操作和資源的完整存取權。此政策也會授予其他必要服務的存取權。這包括列出 Amazon Redshift 叢集、讀取 AWS KMS 中的金鑰和別名，以及管理秘密管理 Secrets Manager 中查詢編輯器 V2 密碼的 AWS 許可。

AmazonRedshiftQueryEditorV2FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRedshiftQueryEditorV2FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 9 月 24 日，世界標準時間 14:06
- 編輯時間：世界標準時間 2024 年 2 月 21 日下午 17 時 20 分
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftQueryEditorV2NoSharing

說明：授予在不共用資源的情況下使用 Amazon Redshift 查詢編輯器 V2 的能力。授與的主體只能讀取、更新和刪除自己的資源，但無法共用它們。此政策也會授予其他必要服務的存取權。這包括列出 Amazon Redshift 叢集和管理秘密管理員中主體的查詢編輯器 V2 AWS 密碼的權限。

`AmazonRedshiftQueryEditorV2NoSharing`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonRedshiftQueryEditorV2NoSharing`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 9 月 24 日，世界標準時間 14:18
- 編輯時間：世界標準時間 2024 年 2 月 21 日 17:25
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftQueryEditorV2ReadSharing

說明：授予在有限共用資源的情況下使用 Amazon Redshift 查詢編輯器 V2 的能力。授予的主體可以讀取，寫入和共享自己的資源。授與的主參與者可以讀取與其專案團隊共用的資源，但無法加以更新。此政策也會授予其他必要服務的存取權。這包括列出 Amazon Redshift 叢集和管理秘密管理員中主體的查詢編輯器 V2 AWS 密碼的權限。

AmazonRedshiftQueryEditorV2ReadSharing是AWS 受管理的策略。

使用此政策

您可以附加AmazonRedshiftQueryEditorV2ReadSharing至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 9 月 24 日，世界標準時間 14:22
- 編輯時間：世界標準時間 2024 年 2 月 21 日下午 17 時 27 分
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
```

```
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
```

```
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
```

```
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftQueryEditorV2ReadWriteSharing

說明：授予與 Amazon Redshift 查詢編輯器 V2 搭配使用資源共用的能力。授予的主體可以讀取，寫入和共享自己的資源。獲得授予的主體可以讀取和更新與其團隊共用的資源。此政策也會授予其他必要服務的存取權。這包括列出 Amazon Redshift 叢集和管理秘密管理員中主體的查詢編輯器 V2 AWS 密碼的權限。

AmazonRedshiftQueryEditorV2ReadWriteSharing是AWS 受管理的策略。

使用此政策

您可以附加AmazonRedshiftQueryEditorV2ReadWriteSharing至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 9 月 24 日，世界標準時間 14:25
- 編輯時間：世界標準時間 2024 年 2 月 21 日下午 5 時 30 分

- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftReadOnlyAccess

說明：透過提供 Amazon Redshift 的 AWS Management Console唯讀存取權。

AmazonRedshiftReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRedshiftReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2024 年 2 月 8 日 00:24
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRedshiftServiceLinkedRolePolicy

說明：允許 Amazon Redshift 代表您呼叫 AWS 服務

AmazonRedshiftServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 9 月 18 日, 世界標準時間 19:19
- 編輯時間：世界標準時間 2024 年 3 月 15 日晚上 8 點
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy

政策版本

策略版本：v13(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRekognitionCustomLabelsFullAccess

說明：此政策指定 Amazon Rekognition 自訂標籤功能所需的重新認知和 s3 許可。

AmazonRekognitionCustomLabelsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRekognitionCustomLabelsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 1 月 8 日, 世界標準時間 19:18
- 編輯時間：2022 年 8 月 16 日，世界標準時間 20:20
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRekognitionFullAccess

說明：存取所有 Amazon Rekognition API

AmazonRekognitionFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRekognitionFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：十一月三十日，世界標準時間下午 2:40
- 編輯時間：2016 年 11 月 30 日，世界標準時間 14:40
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRekognitionReadOnlyAccess

說明：存取所有讀取重新認知 API

AmazonRekognitionReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRekognitionReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：十一月三十日，世界標準時間下午 2:58
- 編輯時間：世界標準時間 2023 年 11 月 8 日 18:30
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRekognitionServiceRole

描述：允許 Rekognition 代表您呼叫 AWS 服務。

AmazonRekognitionServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonRekognitionServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2017 年十一月二十九日，世界標準時間 16:52
- 編輯時間：2017 年十一月二十九日，世界標準時間 16:52
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53AutoNamingFullAccess

描述：提供對所有「Route 53 自動命名」動作的完整存取權。

AmazonRoute53AutoNamingFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53AutoNamingFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 1 月 18 日, 世界標準時間 18:40
- 編輯時間:2018 年 1 月 18 日, 世界標準時間 18:40
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53AutoNamingReadOnlyAccess

描述：提供對所有「Route 53 自動命名」動作的唯讀存取權。

AmazonRoute53AutoNamingReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53AutoNamingReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 1 月 18 日, 3:02 世界標準時間
- 編輯時間:2018 年 1 月 18 日, 3:02 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53AutoNamingRegistrantAccess

描述：提供註冊人層級存取「Route 53 自動命名」動作。

AmazonRoute53AutoNamingRegistrantAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53AutoNamingRegistrantAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 12 日, 世界標準時間 22:33
- 編輯時間：2018 年 3 月 12 日，世界標準時間 22:33
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53DomainsFullAccess

描述：提供對所有 Route53 網域動作的完整存取權，以及建立託管區域以允許建立託管區域作為網域註冊的一部分。

AmazonRoute53DomainsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53DomainsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53DomainsReadOnlyAccess

描述：提供對 Route53 網域清單和動作的存取。

AmazonRoute53DomainsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53DomainsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53FullAccess

描述：通過提供對所有 Amazon Route 53 的完全訪問 AWS Management Console。

AmazonRoute53FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間

- 編輯時間:2018 年十二月二十日, 世界標準時間 21:42
- ARN: arn:aws:iam::aws:policy/AmazonRoute53FullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53ProfilesFullAccess

說明：此政策授予對 Amazon Route 53 設定檔資源的完整存取權。

AmazonRoute53ProfilesFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53ProfilesFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 30 日, 世界標準時間下午 6 時 30 分
- 編輯時間:世界標準時間 2024 年 4 月 30 日, 18:30
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53ProfilesReadOnlyAccess

說明：此政策授予對 Amazon Route 53 設定檔資源的唯讀存取權。

AmazonRoute53ProfilesReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53ProfilesReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 30 日, 世界標準時間 18:29
- 編輯時間:2024 年 4 月 30 日, 世界標準時間 18:29
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53ReadOnlyAccess

描述：通過提供對所有 Amazon Route 53 的只讀訪問 AWS Management Console。

AmazonRoute53ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2016 年 11 月 15 日，世界標準時間 21:15
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53RecoveryClusterFullAccess

說明：提供對 Amazon Route 53 恢復叢集的完整存取

AmazonRoute53RecoveryClusterFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53RecoveryClusterFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 8 月 18 日, 世界標準時間 18:37
- 編輯時間:2021 年 8 月 18 日, 世界標準時間 18:37
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53RecoveryClusterReadOnlyAccess

說明：提供 Amazon Route 53 復原叢集的唯讀存取權

AmazonRoute53RecoveryClusterReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53RecoveryClusterReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 8 月 18 日, 世界標準時間 17:36
- 編輯時間：2022 年 4 月 1 日，世界標準時間 17：37
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53RecoveryControlConfigFullAccess

說明：提供對 Amazon Route 53 恢復控制 Config 的完整訪問權限

AmazonRoute53RecoveryControlConfigFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53RecoveryControlConfigFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 8 月 18 日, 世界標準時間 17:48
- 編輯時間：2021 年 8 月 18 日，世界標準時間 17：48
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53RecoveryControlConfigReadOnlyAccess

說明：提供對 Amazon Route 53 恢復控制 Config 的只讀訪問

AmazonRoute53RecoveryControlConfigReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53RecoveryControlConfigReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 8 月 18 日, 世界標準時間 18:01

- **編輯時間**：世界標準時間 2023 年 10 月 18 日下午 17 時 15 分
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53RecoveryReadinessFullAccess

描述：提供對 Amazon Route 53 恢復準備的完整訪問權限

AmazonRoute53RecoveryReadinessFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53RecoveryReadinessFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 8 月 18 日, 世界標準時間 16:45
- 編輯時間:2021 年 8 月 18 日, 世界標準時間 16:45
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53RecoveryReadinessReadOnlyAccess

說明：提供對 Amazon Route 53 恢復準備的只讀訪問

AmazonRoute53RecoveryReadinessReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53RecoveryReadinessReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 8 月 18 日, 世界標準時間 18:11
- 編輯時間：2021 年 11 月 9 日，世界標準時間 20:14
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53ResolverFullAccess

說明：Route 53 解析程式的完整存取原則

AmazonRoute53ResolverFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53ResolverFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 5 月 30 日, 世界標準時間 18:10
- 編輯時間:2020 年 7 月 17 日, 世界標準時間 19:03
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonRoute53ResolverReadOnlyAccess

說明：Route 53 解析程式的唯讀政策

AmazonRoute53ResolverReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonRoute53ResolverReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 5 月 30 日, 世界標準時間 18:11
- 編輯時間：2019 年 9 月 27 日，世界標準時間 16:37
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonS3FullAccess

說明：透過提供所有值區的完整存取權 AWS Management Console。

AmazonS3FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonS3FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2021 年 9 月 27 日，世界標準時間 20:16
- ARN: arn:aws:iam::aws:policy/AmazonS3FullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonS3ObjectLambdaExecutionRolePolicy

說明：提供 AWS Lambda 函數與 Amazon S3 物件 Lambda 互動的許可。此外，還授與 Lambda 權限，以便寫入 CloudWatch 日誌。

AmazonS3ObjectLambdaExecutionRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonS3ObjectLambdaExecutionRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年 8 月 18 日, 世界標準時間 10:07
- 編輯時間:2021 年 8 月 18 日, 世界標準時間 10:07
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonS3OutpostsFullAccess

說明：提供 Outposts 上的 Amazon S3 的 AWS Management Console完整存取權。

AmazonS3OutpostsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonS3OutpostsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 10 月 2 日, 世界標準時間 17:26
- 編輯時間:2020 年 10 月 2 日, 世界標準時間 17:26
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonS3OutpostsReadOnlyAccess

說明：提供 Outposts 上 Amazon S3 的唯讀存取權，透過 AWS Management Console.

AmazonS3OutpostsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonS3OutpostsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 10 月 2 日, 世界標準時間 18:55
- 編輯時間:2020 年 10 月 2 日, 世界標準時間 18:55
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonS3ReadOnlyAccess

說明：透過提供所有值區的唯讀存取權 AWS Management Console。

AmazonS3ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonS3ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2023 年 8 月 10 日 21:31
- ARN: arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
```

```
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

說明： AWS 服務 目錄服務用於從 Amazon 產品 SageMaker 組合佈建產品的服務角色政策。授予一組相關服務的權限 CodePipeline CodeBuild， CodeCommit包括、 CloudFormation、Glue 等。

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十一月二十七日, 世界標準時間 18:48
- 編輯時間：2022 年 8 月 2 日，世界標準時間 19:12
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerCanvasAIServicesAccess

說明：提供 Amazon SageMaker Canvas 使用 AI 服務的許可，以支援立即使用的 AI 解決方案。隨著 Amazon SageMaker Canvas 增加支援，此政策將為服務新增更多變更許可。

AmazonSageMakerCanvasAIServicesAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerCanvasAIServicesAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 3 月 23 日, 22:36
- 編輯時間：世界標準時間：2023 年 11 月 29 日，下午 4 點 47
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerCanvasBedrockAccess

說明：此政策透過提供 S3 等下游服務的存取權，授予在 SageMaker Canvas 中使用 Amazon 基岩的許可。

AmazonSageMakerCanvasBedrockAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerCanvasBedrockAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間:2024 年 2 月 2 日, 18:37
- 編輯時間：世界標準時間 2024 年 2 月 2 日下午 18:37
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerCanvasDataPrepFullAccess

描述：提供對 Amazon SageMaker 資源和操作的完整存取權，以便在 Canvas 中準備資料。該政策還提供對相關服務（例如 S3，IAM，KMS，RDS， CloudWatch 日誌，Redshift，Athena，Glue EventBridge，Secrets Manager）的選擇訪問權限。此政策應附加至 Amazon SageMaker 網域/使用者設定檔執行角色。

AmazonSageMakerCanvasDataPrepFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerCanvasDataPrepFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 10 月 27 日, 22:56
- 編輯時間:2023 年 12 月 8 日, 02:53 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerCanvasDirectDeployAccess

描述：允許 Amazon SageMaker Canvas 針對透過 Canvas 建立的端點建立、管理和檢視端點詳細資訊。允許 Amazon SageMaker 畫布從 CloudWatch中擷取端點叫用指標。

AmazonSageMakerCanvasDirectDeployAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerCanvasDirectDeployAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略

- **創建時間**:世界標準時間 2023 年 10 月 6 日, 18:11
- **編輯時間**：世界標準時間 2023 年 10 月 6 日 18:11
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerCanvasForecastAccess

說明：此政策授予將 SageMaker Canvas 與 Amazon Forecast 搭配使用所需的許可。

AmazonSageMakerCanvasForecastAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerCanvasForecastAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2022 年 8 月 24 日，世界標準時間 20:04
- 編輯時間：2022 年 8 月 24 日，世界標準時間 20:04
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerCanvasFullAccess

描述：提供對 Amazon SageMaker Canvas 資源和操作的完整存取權。該政策還提供對相關服務的選擇存取權限 (例如 S3、IAM、VPC、ECR、 CloudWatch 日誌、Redshift、Secrets Manager 和 Forecast)。此政策應附加至 Amazon SageMaker 網域/使用者設定檔執行角色。

AmazonSageMakerCanvasFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerCanvasFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：2022 年 9 月 9 日，00:44
- 編輯時間：世界標準時間 2024 年 1 月 24 日 22:01
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerClusterInstanceRolePolicy

說明：此政策授予使用 Amazon SageMaker 叢集通常所需的許可。

AmazonSageMakerClusterInstanceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerClusterInstanceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 11 月 29 日，下午 3:11
- 編輯時間：世界標準時間：2023 年 11 月 29 日，下午 3:11
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerCoreServiceRolePolicy

說明：Amazon SageMaker 核心服務之服務連結角色的受管政策

AmazonSageMakerCoreServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年十二月二十一日, 世界標準時間 21:40
- 編輯時間：2020 年十二月二十一日，世界標準時間 21:40
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerEdgeDeviceFleetPolicy

說明：提供 SageMaker Edge 使用預設雲端連線為客戶建立和管理裝置叢集所需的權限。

AmazonSageMakerEdgeDeviceFleetPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerEdgeDeviceFleetPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年十二月 8 日, 16:17 世界標準時間
- 編輯時間：2020 年 12 月 8 日，世界標準時間 16:17
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerFeatureStoreAccess

描述：提供為 Amazon SageMaker FeatureStore 功能群組啟用離線存放區所需的許可。

AmazonSageMakerFeatureStoreAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerFeatureStoreAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 12 月 1 日, 16:24 世界標準時間
- 編輯時間：世界標準時間：2022 年 12 月 5 日，下午 19 點
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerFullAccess

說明： SageMaker 透過 AWS Management Console 和 SDK 提供對 Amazon 的完整存取權。還提供對相關服務 (例如 S3、ECR、 CloudWatch 日誌) 的選擇存取權限。

AmazonSageMakerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月二十九日，世界標準時間 13:07
- 編輯時間：世界標準時間 2024 年 3 月 29 日 17:35
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFullAccess

政策版本

策略版本：v26(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
```

```
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
```

```
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
```

```
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
```

```
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
```

```
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
```

```
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerGeospatialExecutionRole

描述：此政策提供了對使用 SageMaker 地理空間通常需要的服務的訪問。

AmazonSageMakerGeospatialExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerGeospatialExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：二 ○ 二 ○ 二年十一月三十日，世界標準時
- 編輯時間：世界標準時間 2023 年 5 月 10 日，20:28
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerGeospatialFullAccess

說明：此政策授予允許透過 AWS Management Console 和 SDK 完整存取 Amazon SageMaker 地理空間的許可。

AmazonSageMakerGeospatialFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerGeospatialFullAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：二○二○二年十一月三十

- **編輯時間**：世界標準時間：二 ○ 二二年十一月三十日
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerGroundTruthExecution

說明：提供執行「 SageMaker GroundTruth 標籤」工作所需 AWS 服務的存取權

AmazonSageMakerGroundTruthExecution是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerGroundTruthExecution至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 7 月 9 日, 世界標準時間 19:30
- 編輯時間：2022 年 4 月 29 日，世界標準時間 20:49
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerMechanicalTurkAccess

說明：提供針對任何工作團隊建立 Amazon Augmented AI FlowDefinition 資源的存取權。

AmazonSageMakerMechanicalTurkAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerMechanicalTurkAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 16:19 世界標準時
- 編輯時間：2019 年 12 月 3 日，世界標準時間 16:19
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerModelGovernanceUseAccess

說明：此 AWS 受管政策授予使用所有 Amazon SageMaker 控管功能所需的許可。此政策也提供對相關服務 (例如 S3、KMS) 的選取存取權限。

AmazonSageMakerModelGovernanceUseAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerModelGovernanceUseAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二 ○ 二二年十一月三十日，世界標準時間
- 編輯時間：世界標準時間 2023 年 7 月 17 日 22:31

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

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:ListModelCardExportJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
```

```
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
        "sagemaker:Search",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerModelRegistryFullAccess

描述：這是 Sageemaker 中模型登錄的新受管理原則。此原則是獨立原則，可附加至使用者角色，以存取 Sageemaker 中的模型登錄相關功能。

AmazonSageMakerModelRegistryFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerModelRegistryFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 4 月 13 日，下午 5 時 20 分
- 編輯時間:2023 年 4 月 13 日, 05:20 世界標準時間
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:UpdateModelPackage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "sagemaker:collection"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:collection" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerNotebooksServiceRolePolicy

說明：Amazon SageMaker 筆記型電腦服務連結角色的受管政策

AmazonSageMakerNotebooksServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十月 18 日, 世界標準時間 20:27
- 編輯時間：世界標準時間 2023 年 3 月 9 日下午 18:20
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

說明： AWS ApigateWay 在來自 Amazon 產品 SageMaker 組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。授予一組相關服務的許可，包括 Lambda 和其他服務。

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy是AWS受管理的策略。

使用此政策

您可以附加AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2023 年 8 月 1 日, 下午 3:06
- 編輯時間:世界標準時間 2023 年 8 月 1 日, 下午 3:06
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServi

說明：Amazon 產品 SageMaker 組合中 AWS ServiceCatalog 佈建產品所使用的服務角色政策。AWS CloudFormation 授予相關服務子集的許可，包括 Lambda、ApiGateway 和其他服務。

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy是AWS受管理的策略。

使用此政策

您可以附加AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2023 年 8 月 1 日, 下午 3:06
- 編輯時間:世界標準時間 2023 年 8 月 1 日, 下午 3:06
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

說明： AWS Lambda 在來自 Amazon 產品 SageMaker 組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。授予權限給一組相關服務，包括 Secrets Manager 和其他服務。

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2023 年 8 月 1 日, 世界標準時間 15:05
- 編輯時間:世界標準時間 2023 年 8 月 1 日, 15:05
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerPipelinesIntegrations

說明：此 Amazon 受管政策授予與 SageMaker 模型建立管道中的回呼步驟和 Lambda 步驟搭配使用所需的許可。它被添加到設置 SageMaker Studio 時可以創建的 AmazonSageMaker-ExecutionRole 。它也可以附加到將用於編寫或執行管道的任何其他角色。

AmazonSageMakerPipelinesIntegrations是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerPipelinesIntegrations至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 7 月 30 日, 世界標準時間 16:35
- 編輯時間：世界標準時間 2023 年 2 月 17 日 21:28
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerReadOnly

說明： SageMaker 透過 AWS Management Console 和 SDK 提供對 Amazon 的唯讀存取。

`AmazonSageMakerReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonSageMakerReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月二十九日，世界標準時間 13:07
- 編輯時間：2021 年 12 月 1 日，世界標準時間 16:29
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

說明： AWS ApigateWay 在來自 Amazon 產品 SageMaker 組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。授與一組相關服務 (包括 CloudWatch 記錄和其他服務) 的權限。

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：2022 年 3 月 25 日，04:25
- 編輯時間：2022 年 3 月 25 日，04：25 世界標準時間
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

說明：Amazon 產品 SageMaker 組合中 AWS ServiceCatalog 佈建產品所使用的服務角色政策。AWS CloudFormation 授予相關服務子集 (包括 SageMaker 及其他服務) 的權限。

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy是AWS受管理的策略。

使用此政策

您可以附加AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 3 月 25 日，2022 年 4 月 26 日
- 編輯時間：2022 年 3 月 25 日，04：26 世界標準時間
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

說明：Amazon 產品 SageMaker 組合中 AWS ServiceCatalog 佈建產品所使用的服務角色政策。AWS CodeBuild 授予相關服務子集 (包括 CodePipeline CodeBuild 及其他服務) 的權限。

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 3 月 25 日，2022 年 4 月 27 日
- 編輯時間：2022 年 3 月 25 日，04：27 世界標準時間
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
```

```
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
```

```
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
```

```
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
```

```
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
```

```
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
```

```
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
```

```
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
```

```
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
```

```
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

說明：Amazon 產品 SageMaker 組合中 AWS ServiceCatalog 佈建產品所使用的服務角色政策。AWS CodePipeline 授予相關服務子集 (包括 CodePipeline CodeBuild 及其他服務) 的權限。

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：2022 年 2 月 22 日，09:53
- 編輯時間：2022 年 2 月 22 日，09:53 世界標準時間
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
```

```
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

說明：Amazon 產品 SageMaker 組合中 AWS ServiceCatalog 佈建產品中的 AWS CloudWatch 事件所使用的服務角色政策。授予相關服務子集 (包括 CodePipeline 及其他服務) 的權限。

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：2022 年 2 月 22 日，09:53
- 編輯時間：2022 年 2 月 22 日，09:53 世界標準時間
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

說明： AWS Firehose 在 Amazon 產品 SageMaker 組合中 AWS ServiceCatalog 佈建的產品中使用的服務角色政策。授予一組相關服務的權限，包括 Firehose 及其他服務。

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略

- **創建時間**：世界標準時間：2022 年 2 月 22 日，09:54
- **編輯時間**：2022 年 2 月 22 日（世界標準時間）09:54
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

說明： AWS Glue 在 Amazon 產品 SageMaker 組合中 AWS ServiceCatalog 佈建的產品中使用的服務角色政策。授予一組相關服務的許可，包括 Glue、S3 和其他服務。

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：2022 年 2 月 22 日，09:51
- 編輯時間：2022 年 8 月 26 日，世界標準時間 19:13
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

說明： AWS Lambda 在來自 Amazon 產品 SageMaker 組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。授予一組相關服務的許可，包括 ECR、S3 和其他服務。

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2022 年 4 月 4 日，世界標準時間 16:34
- 編輯時間：2022 年 4 月 4 日，世界標準時間 16:34
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
```

```
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
```

```
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
```

```
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
```

```
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
```

```
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
```

```
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:algorithm/*",
        "arn:aws:sagemaker:*:*:app-image-config/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:automl-job/*",
        "arn:aws:sagemaker:*:*:code-repository/*",
        "arn:aws:sagemaker:*:*:compilation-job/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
        "arn:aws:sagemaker:*:*:device-fleet/*",
        "arn:aws:sagemaker:*:*:edge-packaging-job/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:experiment/*",
        "arn:aws:sagemaker:*:*:experiment-trial/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:feature-group/*",
        "arn:aws:sagemaker:*:*:human-loop/*",
        "arn:aws:sagemaker:*:*:human-task-ui/*",
        "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
        "arn:aws:sagemaker:*:*:image/*",
        "arn:aws:sagemaker:*:*:image-version/*/*",
        "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
        "arn:aws:sagemaker:*:*:labeling-job/*",
        "arn:aws:sagemaker:*:*:model/*",
```

```
        "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
        "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:monitoring-schedule/*",
        "arn:aws:sagemaker:*:*:notebook-instance/*",
        "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
```

```
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSecurityLakeAdministrator

描述：提供對 Amazon 安全湖的完整存取權，以及管理安全湖所需的相關服務。

AmazonSecurityLakeAdministrator是AWS 受管理的策略。

使用此政策

您可以附加AmazonSecurityLakeAdministrator至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 5 月 30 日, 世界標準時間 22:04
- 編輯時間：世界標準時間 2024 年 2 月 23 日，16:01
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",
        "events:ListApiDestinations",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagingSecurityLakeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaCreateFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AllowLambdaAddPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringEquals" : {
          "lambda:Principal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "glue:CreateTable",
        "glue:GetTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule",
        "events:CreateApiDestination",
        "events:CreateConnection",
        "events:UpdateConnection",
        "events:UpdateApiDestination",
        "events:DeleteConnection",
        "events:DeleteApiDestination",
        "events:ListTargetsByRule",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonSecurityLake*",
        "arn:aws:events:*:*:rule/SecurityLake*",
        "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
        "arn:aws:events:*:*:connection/AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs:DeleteQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsCmkGrantForSecurityLake",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "GenerateDataKey",
            "RetireGrant",
            "Decrypt"
          ]
        }
      }
    },
    {
      "Sid" : "AllowEnablingQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:ResourceArn" : [
            "arn:aws:glue:*:*:catalog",
            "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
            "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowConfiguringQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:GetResourceShares",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "LakeFormation*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
```

```
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOnboardingToSecurityLakeDependencies",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "securitylake.amazonaws.com",
            "lakeformation.amazonaws.com",
            "apidestinations.events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowRolePolicyActionsforSubscibersandSources",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowRegisterS3LocationInLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PutRolePolicy",
        "iam:GetRolePolicy"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowIAMActionsByResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRolePolicies",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakes",
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
    },
    {
      "Sid" : "S3ResourcelessReadOnly",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSecurityLakeMetastoreManager

說明：Amazon SecurityLake 元存儲管理器 lambda 的政策，允許訪問雲觀察，S3，Glue 和 SQS。

`AmazonSecurityLakeMetastoreManager`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonSecurityLakeMetastoreManager`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2024 年 1 月 23 日, 世界標準時間 15:26
- 編輯時間:世界標準時間 2024 年 4 月 1 日, 20:04
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSecurityLakePermissionsBoundary

說明：Amazon Security Lake 會為第三方自訂來源建立 IAM 角色，以將資料寫入資料湖，並讓第三方訂閱者使用資料湖中的資料，並在建立這些角色時使用此政策來定義其許可的界限。

AmazonSecurityLakePermissionsBoundary是AWS 受管理的策略。

使用此政策

您可以附加AmazonSecurityLakePermissionsBoundary至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間十一月二十九日，下午 11 時
- 編輯時間：2024 年 5 月 14 日，世界標準時間 20:39
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSESFullAccess

說明：透過提供對 Amazon SES 的完整存取權 AWS Management Console。

AmazonSESFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSESFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/AmazonSESFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSESReadOnlyAccess

說明：透過提供 Amazon SES 的唯讀存取權限 AWS Management Console。

AmazonSESReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSESReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：世界標準時間 5 月 14 日，下午 12:03
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSNSFullAccess

說明：提供完整的 Amazon SNS 存取，透過 AWS Management Console.

AmazonSNSFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSNSFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/AmazonSNSFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSNSReadOnlyAccess

說明：透過提供 Amazon SNS 的唯讀存取權限 AWS Management Console。

AmazonSNSReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSNSReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSNSRole

說明：Amazon SNS 服務角色的預設政策。

AmazonSNSRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonSNSRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSQSFullAccess

說明：可透過. AWS Management Console

AmazonSQSFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSQSFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSQSReadOnlyAccess

說明：提供 Amazon SQS 的唯讀存取權，透過 AWS Management Console.

AmazonSQSReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSQSReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間:2023 年 6 月 15 日, 世界標準時間 15:37
- ARN: arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMAutomationApproverAccess

描述：提供檢視自動化執行的存取權，並將核准決策傳送至等待核准的自動化

AmazonSSMAutomationApproverAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSSMAutomationApproverAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 8 月 7 日, 世界標準時間 23:07
- 編輯時間:2017 年 8 月 7 日, 世界標準時間 23:07
- ARN: arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMAutomationRole

說明：提供 EC2 自動化服務的許可，以執行自動化文件中定義的活動

AmazonSSMAutomationRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonSSMAutomationRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一六年十二月五日, 世界標準時間 22
- 編輯時間:2017 年 7 月 24 日, 世界標準時間 23:29

- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMDirectoryServiceAccess

說明：此原則允許 SSM 代理程式代表客戶存取 Directory Service，以便加入受管理執行個體的網域。

AmazonSSMDirectoryServiceAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSSMDirectoryServiceAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 3 月 15 日, 世界標準時間 17:44
- 編輯時間：2019 年 3 月 15 日，世界標準時間 17:44
- ARN: arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMFullAccess

描述：提供對 Amazon SSM 的完整存取權。

AmazonSSMFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSSMFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 5 月 29 日, 17:39 世界標準時間
- 編輯時間：2019 年 11 月 20 日，世界標準時間 20:08
- ARN: arn:aws:iam::aws:policy/AmazonSSMFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMMaintenanceWindowRole

說明：要用於 EC2 維護時段的服務角色

AmazonSSMMaintenanceWindowRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonSSMMaintenanceWindowRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一六年十二月 1 日, 世界標準時間 15:
- 編輯時間：2019 年 7 月 27 日，世界標準時間 00:16
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
```

```
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMManagedEC2InstanceDefaultPolicy

說明：此政策可在 EC2 執行個體上啟用 AWS Systems Manager 功能。

`AmazonSSMManagedEC2InstanceDefaultPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonSSMManagedEC2InstanceDefaultPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 30 日，世界標準時間 20:54
- 編輯時間：2022 年 8 月 30 日，世界標準時間 20:54
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMManagedInstanceCore

說明：Amazon EC2 角色啟用 AWS Systems Manager 服務核心功能的政策。

AmazonSSMManagedInstanceCore是AWS 受管理的策略。

使用此政策

您可以附加AmazonSSMManagedInstanceCore至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 3 月 15 日, 世界標準時間 17:22
- 編輯時間：2019 年 5 月 23 日，世界標準時間 16:54
- ARN: arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMPatchAssociation

說明：提供修正程式關聯作業之子項執行處理的存取權。

AmazonSSMPatchAssociation是AWS 受管理的策略。

使用此政策

您可以附加AmazonSSMPatchAssociation至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 13 日, 世界標準時間 16:00
- 編輯時間:2020 年 5 月 13 日, 世界標準時間 16:00
- ARN: arn:aws:iam::aws:policy/AmazonSSMPatchAssociation

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMReadOnlyAccess

描述：提供對 Amazon SSM 的唯讀存取權限。

AmazonSSMReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSSMReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 5 月 29 日, 世界標準時間 17:44
- 編輯時間：2015 年 5 月 29 日，世界標準時間 17:44
- ARN: arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSSMServiceRolePolicy

說明：可讓您存取 Amazon SSM 所管理或使用的 AWS 資源

AmazonSSMServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年十一月十三日，世界標準時間 19:20
- 編輯時間：2022 年 9 月 14 日，世界標準時間 19:46
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
```

```
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:SelectResourceConfig"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeCases"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeComplianceByResource",
        "config:DescribeRemediationConfigurations",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStackSets",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DeleteStackInstances",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonSumerianFullAccess

描述：提供對 Amazon Sumerian 的完整訪問權限。

AmazonSumerianFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonSumerianFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 4 月 24 日, 世界標準時間 20:14
- 編輯時間:2018 年 4 月 24 日, 世界標準時間 20:14
- ARN: arn:aws:iam::aws:policy/AmazonSumerianFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTextractFullAccess

說明：訪問所有 Amazon Textract API

AmazonTextractFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonTextractFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十八日, 世界標準時間 19:07
- 編輯時間：2018 年十一月二十八日，世界標準時間 19:07
- ARN: arn:aws:iam::aws:policy/AmazonTextractFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTextractServiceRole

描述：允許 Textract 代表您呼叫 AWS 服務。

AmazonTextractServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AmazonTextractServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年十一月二十八日, 世界標準時間 19:12
- 編輯時間：2018 年十一月二十八日，世界標準時間 19:12
- ARN: arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTimestreamConsoleFullAccess

說明：提供使用管理 Amazon Timestream 的 AWS Management Console完整存取權。請注意，此原則也會授與特定 KMS 作業的權限，以及管理儲存查詢的作業。如果使用客戶管理的 CMK，請參閱文件以瞭解所需的其他權限。

AmazonTimestreamConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonTimestreamConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 9 月 30 日, 世界標準時間 21:47
- 編輯時間：世界標準時間 2022 年 2 月 1 日晚上 9 時 37 分
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTimestreamFullAccess

描述：提供對 Amazon Timestream 的完整訪問權限。請注意，此原則也會授與特定 KMS 作業存取權。如果使用客戶管理的 CMK，請參閱文件以瞭解所需的其他權限。

AmazonTimestreamFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonTimestreamFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 9 月 30 日, 世界標準時間 21:47
- 編輯時間：2021 年十一月二十六日，世界標準時間 23:42
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTimestreamInfluxDBFullAccess

說明：提供建立、更新、刪除和列出 Amazon Timestream InfluxDB 執行個體的完整管理存取權，以及建立和列出參數群組。請參閱文檔以獲取所需的其他權限。

AmazonTimestreamInfluxDBFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonTimestreamInfluxDBFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2024 年 3 月 14 日, 22:53
- 編輯時間：世界標準時間 2024 年 3 月 14 日 22:53
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTimestreamInfluxDBServiceRolePolicy

說明：提供建立、更新、刪除和列出 Amazon Timestream InfluxDB 執行個體的完整管理存取權，以及建立和列出參數群組。請參閱文檔以獲取所需的其他權限。

AmazonTimestreamInfluxDBServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2024 年 3 月 14 日，18:53
- 編輯時間：世界標準時間 2024 年 3 月 14 日下午 18:53
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTimestreamReadOnlyAccess

說明：提供 Amazon Timestream 的唯讀存取權限。原則也提供取消任何執行中查詢的權限。如果使用客戶管理的 CMK，請參閱文件以瞭解所需的其他權限。

AmazonTimestreamReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonTimestreamReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 9 月 30 日, 世界標準時間 21:47
- 編輯時間：世界標準時間 2023 年 2 月 28 日下午 18:22
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
```

```
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTranscribeFullAccess

說明：提供對 Amazon Transcribe 操作的完全訪問

AmazonTranscribeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonTranscribeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 4 月 4 日, 世界標準時間 16:06
- 編輯時間:2018 年 4 月 4 日, 世界標準時間 16:06
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonTranscribeReadOnlyAccess

說明：提供對 Amazon Transcribe 的只讀操作的訪問

AmazonTranscribeReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonTranscribeReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 4 月 4 日, 16:05 世界標準時間
- 編輯時間：2018 年 4 月 4 日，世界標準時間 16:05
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonVPCCrossAccountNetworkInterfaceOperations

描述：提供建立網路介面並將其附加至跨帳戶資源的存取權

AmazonVPCCrossAccountNetworkInterfaceOperations是AWS 受管理的策略。

使用此政策

您可以附加AmazonVPCCrossAccountNetworkInterfaceOperations至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 7 月 18 日, 世界標準時間 20:47
- 編輯時間：世界標準時間 2023 年 9 月 25 日，下午 3:12
- ARN: arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonVPCFullAccess

說明：提供完整的 Amazon VPC 存取權，透過 AWS Management Console.

AmazonVPCFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonVPCFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間:世界標準時間 2024 年 2 月 8 日, 16:03
- ARN: arn:aws:iam::aws:policy/AmazonVPCFullAccess

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

描述：提供描述 AWS 資源、執行網路存取分析器，以及建立或刪除網路深入解析存取範圍和網路深入解析存取範圍分析標籤的權限。

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonVPCNetworkAccessAnalyzerFullAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 6 月 15 日, 世界標準時間 22:56
- 編輯時間：世界標準時間 2024 年 5 月 15 日晚上 9 時 40 分
- ARN: arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonVPCReachabilityAnalyzerFullAccessPolicy

描述：提供描述 AWS 資源、執行可 Reachability Analyzer，以及建立或刪除網路深入解析和網路洞見分析標籤的權限。

AmazonVPCReachabilityAnalyzerFullAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonVPCReachabilityAnalyzerFullAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 6 月 14 日, 世界標準時間 20:12
- 編輯時間:2024 年 5 月 15 日, 世界標準時間 20:47
- ARN: arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

說明：此政策附加至角色 IAM RoleForReachabilityAnalyzerCrossAccountResourceAccess。當管理帳戶啟用可 Reachability Analyzer 的受信任存取時，此角色會部署到組織中的成員帳戶。它提供了使用「可連接 Reachability Analyzer」控制台查看組織中各個資源的權限。

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy是AWS 受管理的策略。

使用此政策

您可以附加AmazonVPCReachabilityAnalyzerPathComponentReadPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 5 月 1 日, 世界標準時間 20:38
- 編輯時間:2023 年 5 月 1 日, 世界標準時間 20:38
- ARN: arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonVPCReadOnlyAccess

說明：透過提供對 Amazon VPC 的 AWS Management Console唯讀存取權。

AmazonVPCReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonVPCReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41

- **編輯時間**：世界標準時間 2024 年 2 月 8 日下午 17 時 08 分
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkDocsFullAccess

描述： WorkDocs 通過提供對 Amazon 的完全訪問 AWS Management Console

`AmazonWorkDocsFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonWorkDocsFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 16 日, 世界標準時間 23:05
- 編輯時間:2020 年 4 月 16 日, 世界標準時間 23:05
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkDocsReadOnlyAccess

說明： WorkDocs 通過 Amazon 提供對亞馬遜的只讀訪問 AWS Management Console

AmazonWorkDocsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkDocsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 1 月 8 日, 23:49 世界標準時間
- 編輯時間:2020 年 1 月 8 日, 世界標準時間 23:49
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkMailEventsServiceRolePolicy

說明：啟用 Amazon WorkMail 活動所使用或管理的資源 AWS 服務 和存取權

`AmazonWorkMailEventsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 4 月 16 日, 16:52 世界標準時間
- 編輯時間：2019 年 4 月 16 日，世界標準時間 16:52
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkMailFullAccess

說明：提供 Directory Service WorkMail、SES、EC2 和 KMS 中繼資料的完整存取權限。

AmazonWorkMailFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkMailFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2020 年十二月二十一日，世界標準時間 14:13
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailFullAccess

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkMailMessageFlowFullAccess

說明： WorkMail 訊息流程 API 的完整存取權

`AmazonWorkMailMessageFlowFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonWorkMailMessageFlowFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 2 月 11 日, 世界標準時間 11:08
- 編輯時間：2021 年 2 月 11 日，世界標準時間 11:08
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workmailmessageflow:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkMailMessageFlowReadOnlyAccess

說明： GetRawMessageContent API WorkMail 訊息的唯讀存取權

AmazonWorkMailMessageFlowReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkMailMessageFlowReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 1 月 28 日, 世界標準時間 12:40
- 編輯時間:2021 年 1 月 28 日, 世界標準時間 12:40
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkMailReadOnlyAccess

描述：提供 WorkMail 和 SES 的唯讀存取權。

AmazonWorkMailReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkMailReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間

- 編輯時間:2019 年 7 月 25 日, 世界標準時間 8:24
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkSpacesAdmin

說明：提供透過 AWS SDK 和 CLI 存取 Amazon WorkSpaces 管理動作的功能。

AmazonWorkSpacesAdmin是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkSpacesAdmin至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 9 月 22 日, 世界標準時間 22:21
- 編輯時間：世界標準時間 2023 年 8 月 3 日 23:57
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkSpacesApplicationManagerAdminAccess

說明：提供管理員存取權，以在 Amazon 應用程式管理員中封裝 WorkSpaces 應用程式

AmazonWorkSpacesApplicationManagerAdminAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkSpacesApplicationManagerAdminAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- 創建時間:2015 年 4 月 9 日, 14:03 世界標準時間
- 編輯時間:2015 年 4 月 9 日, 14:03 世界標準時間
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkspacesPCAAccess

描述：此受管理的原則可提供您的 Certificate Manager Private CA 資源的完整管理存取權，以 AWS 帳戶 進行 AWS 憑證型驗證。

`AmazonWorkspacesPCAAccess`是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkspacesPCAAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：2022 年十一月八日，00:25
- 編輯時間：2022 年十一月八日，世界標準時間 00:25
- ARN: arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkSpacesSelfServiceAccess

說明：提供 Amazon WorkSpaces 後端服務的存取權，以執行工作區自助服務動作

`AmazonWorkSpacesSelfServiceAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmazonWorkSpacesSelfServiceAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 27 日, 世界標準時間 19:22
- 編輯時間：2019 年 6 月 27 日，世界標準時間 19:22
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkSpacesServiceAccess

描述：提供客戶帳戶存取 AWS WorkSpaces 服務以啟動「工作區」。

AmazonWorkSpacesServiceAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkSpacesServiceAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 27 日, 世界標準時間 19:19
- 編輯時間：2020 年 3 月 18 日，世界標準時間 23:32
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkSpacesWebReadOnly

說明：透過 AWS Management Console、開發套件和 CLI 提供對 Amazon WorkSpaces 網路及其相依性的唯讀存取。

AmazonWorkSpacesWebReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AmazonWorkSpacesWebReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 11 月 30 日，世界標準時間 14:20
- 編輯時間：2022 年 11 月 2 日，世界標準時間 20:20
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonWorkSpacesWebServiceRolePolicy

說明：允許訪問 AWS 服務 和由 Amazon WorkSpaces 網絡使用或管理的資源

AmazonWorkSpacesWebServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年十一月三十日, 世界標準時間 13:15
- 編輯時間：2022 年十二月十五日，世界標準時間 22:46
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonZocaloFullAccess

描述：提供對 Amazon Zocalo 的完全訪問權限。

AmazonZocaloFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonZocaloFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/AmazonZocaloFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmazonZocaloReadOnlyAccess

說明：提供對 Amazon Zocalo 的唯讀存取

AmazonZocaloReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AmazonZocaloReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AmplifyBackendDeployFullAccess

說明：提供擴大完整存取權限AWS AppSync，以透過 AWS 雲端 開發套件 (CDK) 部署 Amplify 後端資源 (Amazon Cognito、Amazon S3 和其他相關服務)AWS

`AmplifyBackendDeployFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AmplifyBackendDeployFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零二一年十月六日, 21:32 世界標準時間
- 編輯時間：世界標準時間 2024 年 4 月 17 日下午 4 點
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

APIGatewayServiceRolePolicy

描述：允許 API Gateway 代表客戶管理相關聯的 AWS 資源。

APIGatewayServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 10 月 20 日, 世界標準時間 17:23
- 編輯時間:2021 年 7 月 12 日, 世界標準時間 22:24
- ARN: arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AppIntegrationsServiceLinkedRolePolicy

描述： AppIntegrations 允許代表您管理 AppFlow 資源和發佈 CloudWatch 指標資料。

AppIntegrationsServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2022 年 9 月 30 日，世界標準時間 19:42
- 編輯時間：2022 年 9 月 30 日，世界標準時間 19:42
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ApplicationAutoScalingForAmazonAppStreamAccess

說明：為 Amazon 啟用應用程式自動調度資源的政策 AppStream

`ApplicationAutoScalingForAmazonAppStreamAccess`是AWS 受管理的策略。

使用此政策

您可以附加`ApplicationAutoScalingForAmazonAppStreamAccess`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 2 月 6 日, 21:39 世界標準時間
- 編輯時間：2017 年 2 月 6 日，世界標準時間 21:39
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

描述：啟用「應用 Application Discovery Service 連續匯出」功能所使用或管理的資源 AWS 服務 和存取權

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 8 月 9 日, 世界標準時間 20:22
- 編輯時間:2018 年 8 月 13 日, 世界標準時間 22:31
- ARN: arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AppRunnerNetworkingServiceRolePolicy

描述：允許 AWS AppRunner 網路代表您管理相關 AWS 資源。

AppRunnerNetworkingServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2022 年 1 月 12 日, 21:02

- **編輯時間**：世界標準時間 2022 年 1 月 12 日晚上 9 時 02 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AppRunnerServiceRolePolicy

描述：允 AWS AppRunner 許代表您管理相關 AWS 資源。

AppRunnerServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間**:2021 年 5 月 14 日, 世界標準時間 19:15
- **編輯時間**：2021 年 5 月 14 日，世界標準時間 19:15
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AutoScalingConsoleFullAccess

描述：提供透過「Auto Scaling 整比例」的完整存取權 AWS Management Console。

`AutoScalingConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AutoScalingConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 12 日, 世界標準時間 19:43
- 編輯時間:2018 年 2 月 6 日, 世界標準時間 23:15
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AutoScalingConsoleReadOnlyAccess

描述：透過提供「Auto Scaling」的唯讀存取權 AWS Management Console。

AutoScalingConsoleReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AutoScalingConsoleReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 12 日, 世界標準時間 19:48
- 編輯時間：2017 年 1 月 12 日，世界標準時間 19:48
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AutoScalingFullAccess

描述：提供對 Auto Scaling 整比例的完整存取權。

AutoScalingFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AutoScalingFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 12 日, 世界標準時間 19:31
- 編輯時間:2018 年 2 月 6 日, 世界標準時間 21:59
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AutoScalingNotificationAccessRole

描述： AutoScaling 通知存取服務角色的預設原則。

AutoScalingNotificationAccessRole是AWS 受管理的策略。

使用此政策

您可以附加AutoScalingNotificationAccessRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AutoScalingReadOnlyAccess

描述：提供「Auto Scaling」的唯讀存取。

AutoScalingReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AutoScalingReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 12 日, 世界標準時間 19:39
- 編輯時間：2017 年 1 月 12 日，世界標準時間 19:39
- ARN: arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AutoScalingServiceRolePolicy

描述：啟用 Auto Scaling 所使用或管理的資源的存取 AWS 服務 和資源

`AutoScalingServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 1 月 8 日, 23:10 世界標準時間
- 編輯時間：世界標準時間 2024 年 2 月 29 日 17:48
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWS_ConfigRole

描述：設 AWS Config 服務角色的預設原則。提供 AWS Config 追蹤 AWS 資源變更所需的權限。

AWS_ConfigRole是AWS 受管理的策略。

使用此政策

您可以附加AWS_ConfigRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2020 年 9 月 15 日, 世界標準時間 20:30
- 編輯時間：世界標準時間 2024 年 2 月 22 日晚上 9 時 19 分
- ARN: arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

政策版本

策略版本：v30(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
```

```
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "apigateway:GET",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
```

```
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
```

```
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
```

```
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
```

```
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
```

```
        "connect:DescribeRule",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
```

```
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
```

```
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
```

```
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
```

```
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
```

```
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
```

```
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
```

```
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
```

```
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
```

```
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
```

```
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
```

```
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
```

```
        "kafkaconnect:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
```

```
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
```

```
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListFlows",
        "mediaconnect:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
```

```
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
```

```
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
```

```
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
```

```
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
```

```
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
```

```
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
```

```
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
```

```
        "sagemaker:ListProjects",
        "sagemaker:ListTags",
        "sagemaker:ListWorkteams",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
```

```
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
```

```
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
```

```
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAccountActivityAccess

描述：允許使用者存取「帳戶活動」頁面。

AWSAccountActivityAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAccountActivityAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：世界標準時間 2023 年 3 月 7 日下午 17 時 02 分
- ARN: arn:aws:iam::aws:policy/AWSAccountActivityAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAccountManagementFullAccess

描述：提供 AWS 帳戶管理的完整存取權。

AWSAccountManagementFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAccountManagementFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 9 月 30 日, 世界標準時間 23:20
- 編輯時間：2021 年 9 月 30 日，世界標準時間 23:20
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAccountManagementReadOnlyAccess

說明：提供 AWS 帳戶管理的唯讀存取權

AWSAccountManagementReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAccountManagementReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 9 月 30 日, 世界標準時間 23:29
- 編輯時間：2021 年 9 月 30 日，世界標準時間 23:29
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "account:Get*",
        "account:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAccountUsageReportAccess

描述：允許使用者存取「帳戶使用報告」頁面。

AWSAccountUsageReportAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAccountUsageReportAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/AWSAccountUsageReportAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAgentlessDiscoveryService

描述：提供無探查代理程式連接器的存取權，以向 AWS 應用程式探索服務註冊。

AWSAgentlessDiscoveryService是AWS 受管理的策略。

使用此政策

您可以附加AWSAgentlessDiscoveryService至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2016 年 8 月 2 日, 01:35 世界標準時間

- 編輯時間:2020 年 2 月 24 日, 世界標準時間 23:08
- ARN: arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppFabricFullAccess

說明：提供對 AWS AppFabric 服務的完整存取權，以及 S3、Kinesis、KMS 等相依服務的唯讀存取權。

AWSAppFabricFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppFabricFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 6 月 27 日, 世界標準時間 19:51
- 編輯時間：2023 年 6 月 27 日，世界標準時間 19:51
- ARN: arn:aws:iam::aws:policy/AWSAppFabricFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppFabricReadOnlyAccess

描述：提供對 AWS AppFabric

AWSAppFabricReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppFabricReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 6 月 27 日, 世界標準時間 19:52
- 編輯時間:2023 年 6 月 27 日, 世界標準時間 19:52
- ARN: arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppFabricServiceRolePolicy

描述：提供您 AppFabric 存取 AWS 資源的代表

AWSAppFabricServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2023 年 6 月 26 日, 世界標準時間 21:07
- 編輯時間：世界標準時間 2023 年 6 月 26 日晚上 7 時 7 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingAppStreamFleetPolicy

說明：授與「Application Auto Scaling」權限的原則，以便存取 AppStream 和 CloudWatch.

AWSApplicationAutoscalingAppStreamFleetPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間:**2017 年 10 月 20 日, 世界標準時間 19:04
- **編輯時間**：2017 年 10 月 20 日，世界標準時間 19:04
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingCassandraTablePolicy

說明：原則授與權限給 Application Auto Scaling，以存取 Cassandra 和. CloudWatch

AWSApplicationAutoscalingCassandraTablePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 3 月 18 日, 世界標準時間 22:49
- 編輯時間:2020 年 3 月 18 日, 世界標準時間 22:49
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingComprehendEndpointPolicy

說明：原則授與權限給 Application Auto Scaling 資源調整，以存取 Comprehend 和. CloudWatch

`AWSApplicationAutoscalingComprehendEndpointPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月十四日, 18:39 世界時間
- 編輯時間：2019 年 11 月 14 日，世界標準時間 18:39
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoScalingCustomResourcePolicy

說明：將權限授與應用程式自動調整規模的原則，以存取 ApigateWay 和自 CloudWatch 訂資源擴展

AWSApplicationAutoScalingCustomResourcePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 6 月 4 日, 世界標準時間 23:22
- 編輯時間:2018 年 6 月 4 日, 世界標準時間 23:22
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingDynamoDBTablePolicy

說明：將權限授與應用程式自動擴展以存取 DynamoDB 和. CloudWatch

AWSApplicationAutoscalingDynamoDBTablePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：二零一七年十月二十日 21:34 世界標準時間
- 編輯時間：2017 年 10 月 20 日，世界標準時間 21:34
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

說明：將權限授與應用程式自動擴展以存取 EC2 競價型叢集和 CloudWatch.

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 10 月 25 日, 世界標準時間 18:23
- 編輯時間:2017 年 10 月 25 日, 世界標準時間 18:23
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingECSServicePolicy

說明：將權限授與應用程式自動擴展以存取 EC2 容器服務和 CloudWatch.

AWSApplicationAutoscalingECSServicePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 10 月 25 日, 23:53 世界標準時間
- 編輯時間：2017 年 10 月 25 日，世界標準時間 23:53
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingElastiCacheRGPolicy

說明：授予 Application Auto Scaling 權限的政策，以存取 Amazon ElastiCache 和 Amazon CloudWatch。

AWSApplicationAutoscalingElastiCacheRGPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 8 月 17 日, 世界標準時間 23:41
- 編輯時間:2021 年 8 月 17 日, 世界標準時間 23:41
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingEMRInstanceGroupPolicy

說明：將權限授與應用程式自動調整以存取彈性對應減少和 CloudWatch.

AWSApplicationAutoscalingEMRInstanceGroupPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年十月二十六日, 世界標準時間 00:57
- 編輯時間：2017 年十月二十六日，世界標準時間 00:57
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingKafkaClusterPolicy

說明：原則授與權限給 Application Auto Scaling 資源調整，以存取 Apache Kafka 和. CloudWatch

`AWSApplicationAutoscalingKafkaClusterPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- 創建時間:2020 年 8 月 24 日, 世界標準時間 18:36
- 編輯時間:2020 年 8 月 24 日, 世界標準時間 18:36
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingLambdaConcurrencyPolicy

說明：將權限授與應用程式自動擴展以存取 Lambda 和 CloudWatch.

AWSApplicationAutoscalingLambdaConcurrencyPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 10 月 21 日, 世界標準時間 20:04
- 編輯時間：2019 年 10 月 21 日，世界標準時間 20:04
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingNeptuneClusterPolicy

說明：授予 Application Auto Scaling 權限的政策，以存取 Amazon Neptune 和 Amazon CloudWatch。

`AWSApplicationAutoscalingNeptuneClusterPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 9 月 2 日, 世界標準時間 21:14
- 編輯時間：2021 年 9 月 2 日，世界標準時間 21:14
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingRDSClusterPolicy

說明：將權限授與應用程式自動調整資源調整以存取 RDS 和 CloudWatch.

AWSApplicationAutoscalingRDSClusterPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 10 月 17 日, 世界標準時間 17:46

- 編輯時間:2018 年 8 月 7 日, 世界標準時間 19:14
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationAutoscalingSageMakerEndpointPolicy

說明：授與「Application Auto Scaling」權限的原則，以便存取 SageMaker 和 CloudWatch.

`AWSApplicationAutoscalingSageMakerEndpointPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 2 月 6 日, 世界標準時間 19:58
- 編輯時間:2023 年 11 月 13 日, 世界標準時間 18:52
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationDiscoveryAgentAccess

描述：提供探查代理程式向 AWS 應用程式探索服務註冊的存取權。

AWSApplicationDiscoveryAgentAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationDiscoveryAgentAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2016 年 5 月 11 日, 世界標準時間 21:38
- 編輯時間:2020 年 2 月 24 日, 世界標準時間 22:26
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationDiscoveryAgentlessCollectorAccess

描述：允許 Application Discovery Service 無代理程式收集器 auto 更新、註冊及與 Application Discovery Service 通訊

`AWSApplicationDiscoveryAgentlessCollectorAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSApplicationDiscoveryAgentlessCollectorAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 16 日，世界標準時間 21:00
- 編輯時間：2022 年 8 月 16 日，世界標準時間 21:00
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationDiscoveryServiceFullAccess

描述：提供檢視和標記 Ap AWS plication Discovery Service 所維護之組態項目的完整存取權

AWSApplicationDiscoveryServiceFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationDiscoveryServiceFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2016 年 5 月 11 日, 21:30 世界標準時間
- 編輯時間：2019 年 6 月 19 日，世界標準時間 21:21
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationAgentInstallationPolicy

說明：此原則允許安裝「 AWS 複寫代理程式」(搭配「 AWS 應用程式移轉服務」(MGN) 使用，以便將外部伺服器移轉至 AWS。將此政策附加到您在安裝 AWS 複寫代理程式時提供其登入資料的 IAM 使用者或角色。

AWSApplicationMigrationAgentInstallationPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationAgentInstallationPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 6 月 19 日（世界標準時間）
- 編輯時間：世界標準時間：2022 年 9 月 20 日上午 11:21
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationAgentPolicy

描述：此原則允許安裝並使用「 AWS 複寫代理程式」(搭配「 AWS 應用程式移轉服務」(MGN) 使用，將外部伺服器移轉至 AWS。將此政策附加到您在安裝 AWS 複寫代理程式時提供其登入資料的 IAM 使用者或角色。

`AWSApplicationMigrationAgentPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSApplicationMigrationAgentPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 4 月 7 日, 世界標準時間 7 點
- 編輯時間：世界標準時間：2022 年 9 月 20 日，上午 11:13
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationAgentPolicy_v2

說明：此原則允許使用「 AWS 複製代理程式」(搭配「 AWS 應用程式移轉服務」(MGN) 使用，將外部伺服器移轉至 AWS。我們不建議您將此政策附加到 IAM 使用者或角色。

AWSApplicationMigrationAgentPolicy_v2是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationAgentPolicy_v2至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 6 月 6 日，下午 14 點
- 編輯時間：2022 年 6 月 6 日，世界標準時間 14:14
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationConversionServerPolicy

說明：此原則允許應用程式移轉服務 (MGN) 轉換伺服器 (應用程式移轉服務啟動的 EC2 執行個體) 與 MGN 服務通訊。MGN 會將具有此政策的 IAM 角色 (做為 EC2 執行個體設定檔) 附加至 MGN 轉換伺服器，MGN 會在需要時自動啟動和終止該伺服器。我們不建議您將此政策附加到 IAM 使用者或角色。當使用者選擇使用 MGN 主控台、CLI 或 API 啟動測試或切換執行個體時，應用程式移轉服務會使用 MGN 轉換伺服器。

`AWSApplicationMigrationConversionServerPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSApplicationMigrationConversionServerPolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:4 月 7 日, 06:48 世界標準時間
- 編輯時間:2021 年 4 月 7 日, 06:48 世界標準時間

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

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationEC2Access

說明：此政策提供使用應用程式遷移服務 (MGN) 以 EC2 執行個體形式啟動遷移的伺服器所需的 Amazon EC2 操作。將此政策附加到您的 IAM 使用者或角色。

AWSApplicationMigrationEC2Access是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationEC2Access至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 4 月 7 日, 07:05 世界標準時間
- 編輯時間：世界標準時間 2023 年 2 月 6 日下午 4 時 7 分
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationFullAccess

說明：此原則提供 AWS 應用程式移轉服務 (MGN) 之所有公用 API 的權限，以及讀取 KMS 金鑰資訊的權限。將此政策附加到您的 IAM 使用者或角色。

AWSApplicationMigrationFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:4 月 7 日, 06:56 世界標準時間
- 編輯時間:世界標準時間 2023 年 4 月 20 日, 17:28
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationMGHAccess

描述：此原則允許 AWS 應用程式移轉服務 (MGN) 傳送關於使用 MGN 移轉至 AWS Migration Hub (MGH) 之伺服器進度的中繼資料。MGN 會自動建立附加此政策的 IAM 角色，並擔任此角色。我們不建議您將此政策附加到 IAM 使用者或角色。

AWSApplicationMigrationMGHAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationMGHAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年 4 月 7 日, 07:10 世界標準時間
- 編輯時間:2021 年 4 月 7 日, 07:10 世界標準時間

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

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationReadOnlyAccess

說明：此原則會提供「應用程式移轉服務」(MGN) 的所有唯讀公用 API 的權限，以及其他 AWS 服務的一些唯讀 API，才能完全以唯讀使用 MGN 主控台。將此政策附加到 IAM 使用者或角色。

AWSApplicationMigrationReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 4 月 7 日, 07:15 世界標準時間
- 編輯時間：世界標準時間 2023 年 3 月 20 日，08:58
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationReplicationServerPolicy

說明：此原則允許應用程式移轉服務 (MGN) 複寫伺服器 (應用程式移轉服務啟動的 EC2 執行個體) 與 MGN 服務通訊，並在您的. AWS 帳戶應用程式遷移服務會將具有此政策的 IAM 角色 (做為 EC2 執行個體設定檔) 附加至 MGN 複寫伺服器，這些伺服器會視需要由 MGN 自動啟動和終止。MGN 複寫伺服器可用來協助將資料從外部伺服器複寫到 AWS，做為使用 MGN 管理的移轉程序的一部分。我們不建議您將此政策附加到 IAM 使用者或角色。

`AWSApplicationMigrationReplicationServerPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSApplicationMigrationReplicationServerPolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年 4 月 7 日, 07:21 世界標準時間
- 編輯時間:2021 年 4 月 7 日, 07:21 世界標準時間
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationServiceEc2InstancePolicy

描述：此原則允許安裝和使用應用程式移轉服務 (AWS MGN) 所使用的 AWS 複寫代理 AWS 程式來移轉 EC2 (跨區域或跨可用區域) 上執行的來源伺服器。應將具有此政策的 IAM 角色 (做為 EC2 執行個體設定檔) 附加至 EC2 執行個體。

AWSApplicationMigrationServiceEc2InstancePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationServiceEc2InstancePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**:世界標準時間 2023 年 8 月 22 日, 13:19
- **編輯時間**：世界標準時間 2024 年 1 月 3 日下午 2:19
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationServiceRolePolicy

說明：允許 AWS 應用程式移轉服務代表您建立和管理 AWS 資源。

AWSApplicationMigrationServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 4 月 7 日, 06:43 世界標準時間
- 編輯時間：世界標準時間：2023 年 6 月 20 日，09:12

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

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationSSMAccess

描述：此政策可讓您存取 Amazon SSM 操作，以便使用應用程式遷移服務 (MGN) 執行自訂移轉後命令 SSM 文件。將此政策附加到您的 IAM 使用者或角色。

AWSApplicationMigrationSSMAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationSSMAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：二零二二年十一月二十七
- 編輯時間：世界標準時間 2023 年 3 月 20 日上午 10:57
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSApplicationMigrationVCenterClientPolicy

描述：此原則允許安裝和使用 AWS vCenter Client (與 AWS 應用程式移轉服務 (MGN) 搭配使用，將外部伺服器移轉至。 AWS將此政策附加至您在安裝 AWS vCenter 用戶端時提供其登入資料的 IAM 使用者或角色。

AWSApplicationMigrationVCenterClientPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSApplicationMigrationVCenterClientPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 11 月 8 日，世界標準時間 12:53
- 編輯時間：2021 年 11 月 8 日，世界標準時間 12:53
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppMeshEnvoyAccess

說明：用於存取虛擬節點設定的應用程式 Mesh 特使政策。

AWSAppMeshEnvoyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppMeshEnvoyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:二零一九年七月三日, 21:29 世界標準時間**
- **編輯時間:2019 年 7 月 3 日, 世界標準時間 21:29**
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppMeshFullAccess

說明：提供對 AWS App Mesh API 和管理主控台的完整存取權。

AWSAppMeshFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppMeshFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 4 月 16 日, 世界標準時間 17:50
- 編輯時間：2021 年 1 月 7 日，世界標準時間 19:54
- ARN: arn:aws:iam::aws:policy/AWSAppMeshFullAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppMeshPreviewEnvoyAccess

說明：用於存取虛擬節點設定的應用程式網狀預覽特使政策。

AWSAppMeshPreviewEnvoyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppMeshPreviewEnvoyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 8 月 5 日, 23:32 世界標準時間
- 編輯時間：2019 年 8 月 5 日，世界標準時間 23:32
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ],
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppMeshPreviewServiceRolePolicy

說明：啟用 AWS App Mesh 所使用或管理的存取 AWS 服務 和資源

AWSAppMeshPreviewServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 6 月 19 日, 世界標準時間 19:07
- 編輯時間：2019 年 8 月 21 日，世界標準時間 21:06
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppMeshReadOnly

說明：提供 AWS App Mesh API 和管理主控台的唯讀存取權。

AWSAppMeshReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSAppMeshReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 4 月 16 日, 世界標準時間 17:51
- 編輯時間：2021 年 1 月 7 日，世界標準時間 19:53
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppMeshServiceRolePolicy

描述：啟用存取以 AWS 服務 及使用或管理的資源 AWS AppMesh

AWSAppMeshServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 6 月 3 日, 世界標準時間下午 18:30
- 編輯時間:世界標準時間 2023 年 10 月 10 日, 16:46
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppRunnerFullAccess

說明：授予所有「App 執行器」動作的權限。

AWSAppRunnerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppRunnerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：2022 年 1 月 11 日，04:02
- 編輯時間：世界標準時間 2022 年 1 月 11 日 04 時 02 日
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppRunnerReadOnlyAccess

說明：授予列出和檢視 App Runner 資源詳細資料的權限。

AWSAppRunnerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppRunnerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2022 年 2 月 24 日晚上 9 點 24 日
- 編輯時間：世界標準時間 2022 年 2 月 24 日晚上 9 時 24 分
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppRunnerServicePolicyForECRAccess

說明：授與讀取權限給客戶帳戶中 Amazon ECR 資源的 AWS 應用程式執行器服務政策。在創建或更新應用程序運行器服務時傳遞給應用程序運行器的角色中使用它。

AWSAppRunnerServicePolicyForECRAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppRunnerServicePolicyForECRAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年 5 月 14 日, 世界標準時間 19:17
- 編輯時間：2021 年 5 月 14 日，世界標準時間 19:17
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppSyncAdministrator

描述：提供對 AppSync 服務的管理存取權，但不足以透過主控台存取。

AWSAppSyncAdministrator是AWS 受管理的策略。

使用此政策

您可以附加AWSAppSyncAdministrator至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 20 日, 世界標準時間 21:20
- 編輯時間：2019 年 11 月 4 日，世界標準時間 19:23
- ARN: arn:aws:iam::aws:policy/AWSAppSyncAdministrator

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppSyncInvokeFullAccess

說明：提供完整的 AppSync 服務叫用存取權-透過主控台和獨立

AWSAppSyncInvokeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSAppSyncInvokeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 20 日, 世界標準時間 21:21
- 編輯時間：2018 年 3 月 20 日，世界標準時間 21:21
- ARN: arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppSyncPushToCloudWatchLogs

描述：允許 AppSync 將日誌推送到用戶的 CloudWatch 帳戶。

AWSAppSyncPushToCloudWatchLogs是AWS 受管理的策略。

使用此政策

您可以附加AWSAppSyncPushToCloudWatchLogs至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 4 月 9 日, 世界標準時間 19:38
- 編輯時間:2018 年 4 月 9 日, 世界標準時間 19:38
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppSyncSchemaAuthor

描述：提供建立、更新和查詢綱要的存取權。

AWSAppSyncSchemaAuthor是AWS 受管理的策略。

使用此政策

您可以附加AWSAppSyncSchemaAuthor至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 20 日, 世界標準時間 21:21
- 編輯時間：世界標準時間 2023 年 2 月 1 日下午 18:36
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAppSyncServiceRolePolicy

描述：允許存取使用或管理的 AWS 服務和資源 AppSync

AWSAppSyncServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 1 月 21 日, 世界標準時間 19:56
- 編輯時間：2020 年 1 月 21 日，世界標準時間 19:56
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSArtifactAccountSync

描述：允許 AWS Artifact 唯讀存取「Organ AWS izations」中的作業。

AWSArtifactAccountSync是AWS 受管理的策略。

使用此政策

您可以附加AWSArtifactAccountSync至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略

- 創建時間:2018 年 4 月 10 日, 世界標準時間 23:04
- 編輯時間:2018 年 4 月 10 日, 世界標準時間 23:04
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSArtifactReportsReadOnlyAccess

描述：提供「 AWS Artifact」服務報表的唯讀存取權。

AWSArtifactReportsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSArtifactReportsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2024 年 1 月 2 日, 世界標準時間 22:42
- 編輯時間:2024 年 1 月 2 日, 世界標準時間 22:42
- ARN: arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSArtifactServiceRolePolicy

描述：允許 AWS Artifact 透過 AWS 「組織」服務收集組織的相關資訊。

AWSArtifactServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2023 年 8 月 21 日, 世界標準時間 20:27
- 編輯時間：世界標準時間 2023 年 8 月 21 日，20:27
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAuditManagerAdministratorAccess

描述：提供管理存取權，以啟用或停用 AWS Audit Manager、更新設定以及管理評量、控制項和架構

`AWSAuditManagerAdministratorAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSAuditManagerAdministratorAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十一日, 世界標準時間 20:02
- 編輯時間:2024 年 5 月 15 日, 世界標準時間 23:46
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAuditManagerServiceRolePolicy

描述：啟用 AWS 稽核管理員所使用或管理的資源 AWS 服務 與存取權

AWSAuditManagerServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年十二月 8 日, 下午 3:12 世界標準時間
- 編輯時間：2024 年 5 月 9 日，世界標準時間 16:51
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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:ListEntitiesForPolicy",
        "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",
        "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:ListEndpointConfigs",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "sagemaker:DescribeEndpointConfig",
        "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" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${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"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSAutoScalingPlansEC2AutoScalingPolicy

說明：將權限授與 AWS Auto Scaling 的政策，以定期預測容量並為擴展計劃中的 Auto Scaling 群組產生排定的擴展動作

AWSAutoScalingPlansEC2AutoScalingPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 8 月 23 日, 世界標準時間 22:46
- 編輯時間:2018 年 8 月 23 日, 世界標準時間 22:46
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupAuditAccess

說明：此政策授予使用者建立控制項和架構的權限，以定義他們對 AWS Backup 資源和活動的期望，並根據其定義的控制項和架構稽核 AWS Backup 資源和活動。此原則會授與 AWS Config 和類似服務的權限，以說明使用者期望執行稽核。此政策還授予將稽核報告傳遞給 S3 和類似服務的許可，並讓使用者能夠尋找和開啟其稽核報告。

AWSBackupAuditAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupAuditAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 8 月 24 日, 01:02 世界標準時間
- 編輯時間：世界標準時間 2023 年 4 月 10 日晚上 9 時 23 分
- ARN: arn:aws:iam::aws:policy/AWSBackupAuditAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupDataTransferAccess

描述：此原則允許 AWS Backint 代理程式使用 Backup 儲存體平面完成備 AWS 份資料傳輸。將此政策附加至透過 Backint 代理程式執行 SAP HANA 的 EC2 執行個體所承擔的角色。

`AWSBackupDataTransferAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSBackupDataTransferAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二○二二年十一月十日，世界標準時間 22
- 編輯時間：2022 年十一月十日，世界標準時間 22:48
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupFullAccess

說明：此原則適用於 Backup 管理員，可授與 AWS 備份作業的完整存取權，包括建立或編輯備份計劃、指定 AWS 資源給備份計劃、刪除備份以及還原備份。

AWSBackupFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月十八日, 世界標準時間
- 編輯時間：世界標準時間 2023 年 11 月 27 日下午 17 時 33 分
- ARN: arn:aws:iam::aws:policy/AWSBackupFullAccess

政策版本

策略版本：v17(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

說明：提供代表您同步虛擬機器中繼資料的 AWS BackupGateway 權限

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：二零二二年十二月十五日
- 編輯時間：2022 年十二月十五日，世界標準時間 19:43
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupOperatorAccess

描述：此原則授與使用者將 AWS 資源指派給備份計劃、建立隨選備份及還原備份的權限。此原則不允許使用者在建立備份之後建立或編輯備份計劃或刪除排定的備份。

AWSBackupOperatorAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupOperatorAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月十八日, 世界標準時間
- 編輯時間：世界標準時間 2023 年 9 月 6 日晚上 20:45
- ARN: arn:aws:iam::aws:policy/AWSBackupOperatorAccess

政策版本

策略版本：v15(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupOrganizationAdminAccess

描述：此原則適用於使用跨帳戶備份管理來管理組織備份的備份的備份管理員。

AWSBackupOrganizationAdminAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupOrganizationAdminAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 24 日, 世界標準時間 16:23
- 編輯時間：2022 年十一月十八日，世界標準時間 18:26
- ARN: arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupRestoreAccessForSAPHANA

說明：提供 AWS Backup 權限，以在 Amazon EC2 上還原 SAP HANA 的備份

AWSBackupRestoreAccessForSAPHANA是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupRestoreAccessForSAPHANA至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二 ○ 二二年十一月十日，世界標準時間 22
- 編輯時間：2022 年十一月十日，世界標準時間 22:43
- ARN: arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupServiceLinkedRolePolicyForBackup

說明：提供 AWS Backup 權限，以代表您跨 AWS 服務建立備份

AWSBackupServiceLinkedRolePolicyForBackup是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 6 月 2 日, 世界標準時間 23:08
- 編輯時間：世界標準時間 2023 年十二月十五日上午 22 點 6
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup

政策版本

策略版本：v15(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupServiceLinkedRolePolicyForBackupTest

說明：提供 AWS Backup 權限，以代表您跨 AWS 服務建立備份

AWSBackupServiceLinkedRolePolicyForBackupTest是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 5 月 12 日, 世界標準時間 17:37
- 編輯時間:2020 年 5 月 12 日, 世界標準時間 17:37
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupServiceRolePolicyForBackup

說明：提供 AWS Backup 權限，以代表您跨 AWS 服務建立備份

AWSBackupServiceRolePolicyForBackup是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupServiceRolePolicyForBackup至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一九年一月十日, 21:01 世界標準時間
- 編輯時間：世界標準時間 2023 年 12 月 15 日, 22:04
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup

政策版本

策略版本：v18(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
```

```
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "rds:DeleteDBClusterAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
```

```
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
    {
```

```
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EBSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
```

```
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
```

```
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterSnapshot",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
```

```
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
```

```
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupServiceRolePolicyForRestores

說明：提供 AWS Backup 權限，以代表您跨 AWS 服務執行還原。此原則包括建立和刪除 AWS 資源 (例如 EBS 磁碟區、RDS 執行個體和 EFS 檔案系統) 的權限，這些資源是還原程序的一部分。

AWSBackupServiceRolePolicyForRestores是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupServiceRolePolicyForRestores至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2019 年 1 月 12 日，世界標準時間 00:23
- 編輯時間：世界標準時間 2023 年 12 月 15 日, 22:05
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores

政策版本

策略版本：v20(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
```

```
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
```

```
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
```

```
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
```

```
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "DSPermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
```

```
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupServiceRolePolicyForS3Backup

說明：包含 AWS Backup 在任何 S3 儲存貯體中備份資料所需許可的政策。這包括對所有 S3 物件的讀取存取權，以及所有 KMS 金鑰的任何解密存取權。

AWSBackupServiceRolePolicyForS3Backup是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupServiceRolePolicyForS3Backup至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2022 年 2 月 18 日下午 17 時 40 分
- 編輯時間：2022 年 9 月 1 日，世界標準時間下午 16 點 52
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
```

```
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:GetInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutInventoryConfiguration",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:ListAllMyBuckets",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBackupServiceRolePolicyForS3Restore

說明：包含 Backup 將 S3 備 AWS 份還原到儲存貯體所需許可的政策。這包括 DescribeKey 對所有 S3 儲存貯體的讀取/寫入許可，以 GenerateDataKey 及所有 KMS 金鑰的權限。

AWSBackupServiceRolePolicyForS3Restore是AWS 受管理的策略。

使用此政策

您可以附加AWSBackupServiceRolePolicyForS3Restore至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2022 年 2 月 18 日，下午 17 點 39
- 編輯時間：世界標準時間 2023 年 2 月 7 日凌時 06 分
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBatchFullAccess

描述：提供 AWS Batch 資源的完整存取權。

AWSBatchFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBatchFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年十二月六日, 19:35 世界標準時
- 編輯時間：2022 年 10 月 24 日，世界標準時間 16:09
- ARN: arn:aws:iam::aws:policy/AWSBatchFullAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBatchServiceEventTargetRole

描述：針對 AWS Batch Job 提交啟用 CloudWatch 事件目標的原則

AWSBatchServiceEventTargetRole是AWS 受管理的策略。

使用此政策

您可以附加AWSBatchServiceEventTargetRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 2 月 28 日, 世界標準時間 22:31
- 編輯時間:2018 年 2 月 28 日, 世界標準時間 22:31
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBatchServiceRole

說明： AWS Batch 服務角色的政策，允許存取相關服務，包括 EC2、自動調度資源、EC2 容器服務和 Cloudwatch 日誌。

AWSBatchServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AWSBatchServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一六年十二月六日, 19:36 世界標準時
- 編輯時間：世界標準時間 2023 年 12 月 5 日下午 18:49
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

政策版本

策略版本：v13(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBillingConductorFullAccess

描述：使用 AWSBillingConductorFullAccess 受管政策允許完整存取 AWS Billing Conductor (ABC) 主控台和 API。此原則允許使用者列出、建立和刪除 ABC 資源。

AWSBillingConductorFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBillingConductorFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間（世界標準時間）4 月 13 日
- 編輯時間：2022 年 4 月 13 日，世界標準時間 18:02
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBillingConductorReadOnlyAccess

描述：使用受 AWSBillingConductorReadOnlyAccess 管理的政策允許 AWS Billing Conductor (ABC) 主控台和 API 的唯讀存取權。此政策授予檢視和列出所有 ABC 資源的權限。它不包括創建或刪除資源的功能。

AWSBillingConductorReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBillingConductorReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**：2022 年 4 月 13 日，世界標準時間 18:02
- **編輯時間**：2022 年 4 月 13 日，世界標準時間 18:02
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBillingReadOnlyAccess

描述：允許使用者在計費主控台上檢視帳單。

AWSBillingReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBillingReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 27 日, 世界標準時間 20:08
- 編輯時間：世界標準時間 2024 年 1 月 17 日下午 18:15
- ARN: arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
```

```
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

描述：此原則授與控制資 AWS 源的權限。例如，若要啟動和停止 EC2 或 RDS 執行個體，請執行 AWS Systems Manager (SSM) 指令碼。

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM是AWS 受管理的策略。

使用此政策

您可以附加AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 5 月 25 日，世界標準時間 19:03
- 編輯時間：2022 年 5 月 25 日，世界標準時間 19:03
- ARN: arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBudgetsActionsWithAWSResourceControlAccess

摘要：提供「 AWS 預算作業」的完整存取權，包括使用「預算作業」來控制執行 AWS 資源的狀態，AWS Management Console

AWSBudgetsActionsWithAWSResourceControlAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBudgetsActionsWithAWSResourceControlAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十月 15 日, 世界標準時間 17:19
- 編輯時間:2020 年 10 月 15 日, 世界標準時間 17:19
- ARN: arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBudgetsReadOnlyAccess

說明：透過「」提供「 AWS 預算主控台」的唯讀存取權 AWS Management Console。

AWSBudgetsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBudgetsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 10 月 15 日, 世界標準時間 17:18
- 編輯時間:2020 年 10 月 15 日, 世界標準時間 17:18
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBugBustFullAccess

說明：此 IAM 政策授予使用者對 AWS BugBust 主控台的完整存取權

AWSBugBustFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBugBustFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 6 月 24 日, 07:03
- 編輯時間:2021 年 7 月 22 日, 世界標準時間 20:04
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBugBustPlayerAccess

說明：此 IAM 政策授予使用者參與 AWS BugBust 活動的存取權

AWSBugBustPlayerAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSBugBustPlayerAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 6 月 24 日, 07:15 世界標準時間
- 編輯時間：2021 年 6 月 24 日，07:15 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSBugBustServiceRolePolicy

描述：授與代表 AWS BugBust 您存取資源的權限

AWSBugBustServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:6 月 24 日, 06:59 世界標準時間
- 編輯時間:2021 年 6 月 24 日, 06:59 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
```

```
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCertificateManagerFullAccess

描述：提供 Cer AWS tificate Manager (ACM) 的完整存取權

`AWSCertificateManagerFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSCertificateManagerFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年一月二十一日, 下午 17 時 02 分
- 編輯時間:2020 年 8 月 17 日, 世界標準時間 22:18
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCertificateManagerPrivateCAAuditor

描述：提供稽核員存取 Cer AWS tificate Manager 專用憑證授權單位

AWSCertificateManagerPrivateCAAuditor是AWS 受管理的策略。

使用此政策

您可以附加AWSCertificateManagerPrivateCAAuditor至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 23 日, 16:51 世界標準時間
- 編輯時間：2020 年 8 月 17 日, 世界標準時間 22:54
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCertificateManagerPrivateCAFullAccess

描述：提供「Certificate Manager」私有 AWS 憑證授權單位的完整

`AWSCertificateManagerPrivateCAFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSCertificateManagerPrivateCAFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- 創建時間:2018 年 10 月 23 日, 世界標準時間 16:54
- 編輯時間:2018 年 10 月 23 日, 世界標準時間 16:54
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCertificateManagerPrivateCAPrivilegedUser

說明：提供有權限的憑證使用者存取 Cer AWS tificate Manager 專用憑證授權

`AWSCertificateManagerPrivateCAPrivilegedUser`是AWS 受管理的策略。

使用此政策

您可以附加AWSCertificateManagerPrivateCAPrivilegedUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 20 日, 世界標準時間 17:43
- 編輯時間:2019 年 6 月 20 日, 世界標準時間 17:43
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCertificateManagerPrivateCAReadOnly

說明：提供 Certificate Manager 專用 AWS 憑證授權單位的唯讀存取權

AWSCertificateManagerPrivateCAReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSCertificateManagerPrivateCAReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 23 日, 世界標準時間 16:57
- 編輯時間：2020 年 8 月 17 日, 世界標準時間 22:54
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCertificateManagerPrivateCAUser

描述：提供憑證使用者存取 Cer AWS tificate Manager 專用憑證授權單位

`AWSCertificateManagerPrivateCAUser`是AWS 受管理的策略。

使用此政策

您可以附加`AWSCertificateManagerPrivateCAUser`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 23 日, 世界標準時間 16:53
- 編輯時間:2019 年 6 月 20 日, 世界標準時間 17:42
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCertificateManagerReadOnly

描述：提供 Cer AWS tificate Manager (ACM) 的唯讀存取權。

`AWSCertificateManagerReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`AWSCertificateManagerReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年一月二十一日, 下午 17 點 7 分
- 編輯時間：2021 年 3 月 15 日，世界標準時間 16:25
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSChatbotServiceLinkedRolePolicy

描述：C AWS hatbot 使用的服務鏈接角色。

AWSChatbotServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月十八日, 16:39 世界時間
- 編輯時間：2019 年 11 月 18 日，世界標準時間 16:39
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCleanRoomsFullAccess

描述：允許完全存取 AWS 潔淨室資源並存取相關資源 AWS 服務。

AWSCleanRoomsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCleanRoomsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 1 月 12 日, 16:10
- 編輯時間：世界標準時間 2024 年 3 月 21 日，下午 3:35
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
```

```
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickQueryResultsBucketListAll",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SetQueryResultsBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "WriteQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleDisplayQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCleanRoomsFullAccessNoQuerying

描述：允許完整存取 C AWS lean Rooms 資源，但在協同作業中進行查詢和存取相關資源除外 AWS 服務。

AWSCleanRoomsFullAccessNoQuerying是AWS 受管理的策略。

使用此政策

您可以附加AWSCleanRoomsFullAccessNoQuerying至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 1 月 12 日, 16:12
- 編輯時間:2024 年 5 月 14 日, 世界標準時間 18:31
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCleanRoomsMLFullAccess

描述：允許完整存取無 AWS 塵室 ML 資源並存取相關資源 AWS 服務。

AWSCleanRoomsMLFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCleanRoomsMLFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二一年十一月二十九日, 世界標準時間晚
- 編輯時間：世界標準時間 2023 年 11 月 29 日晚上 9 時 02 分
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCleanRoomsMLReadOnlyAccess

描述：允許對 AWS 清潔室 ML 資源進行唯讀存取，以及對相關 AWS 潔淨室資源的唯讀存取

AWSCleanRoomsMLReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCleanRoomsMLReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二一年十一月二十九日, 世界標準時間 20:
- 編輯時間：世界標準時間 2023 年 11 月 29 日晚上 20:55
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCleanRoomsReadOnlyAccess

描述：允許對 AWS 清潔室資源進行唯讀存取，以及對相關 AWS Glue 和 Amazon CloudWatch 日誌資源的唯讀存取權。

AWSCleanRoomsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCleanRoomsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 1 月 12 日, 16:10
- 編輯時間:世界標準時間 2023 年 1 月 12 日, 16:10
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloud9Administrator

描述：提供管理員對 AWS Cloud9 的存取權。

AWSCloud9Administrator是AWS 受管理的策略。

使用此政策

您可以附加AWSCloud9Administrator至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月三十日，世界標準時間 16:17
- 編輯時間：世界標準時間 2023 年 10 月 11 日 12:59
- ARN: arn:aws:iam::aws:policy/AWSCloud9Administrator

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloud9EnvironmentMember

描述：提供受邀進入 AWS Cloud9 共用開發環境的功能。

AWSCloud9EnvironmentMember是AWS 受管理的策略。

使用此政策

您可以附加AWSCloud9EnvironmentMember至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月三十日，世界標準時間 16:18
- 編輯時間：世界標準時間 2023 年 10 月 11 日 12:13
- ARN: arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloud9ServiceRolePolicy

說明： AWS Cloud9 的服務連結角色政策

AWSCloud9ServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年十一月三十日，世界標準時間 13:44
- 編輯時間：世界標準時間 2022 年 1 月 17 日下午 4 時 6 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloud9SSMInstanceProfile

說明：此政策將用於附加角色，讓 Cloud9 使用 SSM 工作階段管理員連線至執行個 InstanceProfile 體

AWSCloud9SSMInstanceProfile是AWS 受管理的策略。

使用此政策

您可以附加AWSCloud9SSMInstanceProfile至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 14 日, 世界標準時間 11:40
- 編輯時間:2020 年 5 月 14 日, 世界標準時間 11:40
- ARN: arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloud9User

描述：提供建立 AWS Cloud9 開發環境和管理擁有環境的權限。

AWSCloud9User是AWS 受管理的策略。

使用此政策

您可以附加AWSCloud9User至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**：2017 年十一月三十日，世界標準時間 16:16
- **編輯時間**：世界標準時間 2023 年 10 月 11 日，13:24
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudFormationFullAccess

描述：提供對的完整存取權 AWS CloudFormation。

AWSCloudFormationFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudFormationFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 7 月 26 日, 世界標準時間 21:50
- 編輯時間：2019 年 7 月 26 日，世界標準時間 21:50
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudFormationReadOnlyAccess

描述：提供 AWS CloudFormation 透過 AWS Management Console.

AWSCloudFormationReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudFormationReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間：2019 年十一月十三日，世界標準時間 17:40
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudFrontLogger

描述：授與 CloudFront 記錄 CloudWatch 檔的寫入權限。

AWSCloudFrontLogger是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 6 月 12 日, 世界標準時間 20:15
- 編輯時間：2019 年十一月二十二日，世界標準時間 19:33
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudHSMFullAccess

描述：提供對所有 CloudHSM 資源的完整存取權。

AWSCloudHSMFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudHSMFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間:2015 年 2 月 6 日, 18:39 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudHSMReadOnlyAccess

描述：提供對所有 CloudHSM 資源的唯讀存取權。

AWSCloudHSMReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudHSMReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間:2015 年 2 月 6 日, 18:39 世界標準時間

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

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudHSMRole

說明： AWS CloudHSM 服務角色的預設政策。

`AWSCloudHSMRole`是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudHSMRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudMapDiscoverInstanceAccess

描述：提供對 AWS 雲端 映探索 API 的存取權。

AWSCloudMapDiscoverInstanceAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudMapDiscoverInstanceAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2018 年十一月二十九日，世界標準時間 00:02
- 編輯時間：世界標準時間 2023 年 9 月 20 日晚上 9 時 48 分
- ARN: arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudMapFullAccess

描述：提供對所有「對 AWS 雲端 映」動作的完整存取權。

AWSCloudMapFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudMapFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十八日, 世界標準時間 23:57
- 編輯時間:2020 年 7 月 29 日, 世界標準時間 19:15
- ARN: arn:aws:iam::aws:policy/AWSCloudMapFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudMapReadOnlyAccess

描述：提供對所有 AWS 雲端 Map 動作的唯讀存取權。

AWSCloudMapReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudMapReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十八日, 世界標準時間 23:45
- 編輯時間：世界標準時間 2023 年 9 月 20 日晚上 9 時 47 分
- ARN: arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudMapRegisterInstanceAccess

描述：提供註冊者層級存取「 AWS 雲端 地圖」動作。

AWSCloudMapRegisterInstanceAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudMapRegisterInstanceAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2018 年十一月二十九日，世界標準時間 00:04
- 編輯時間：世界標準時間 2023 年 9 月 20 日晚上 9 時 47 分
- ARN: arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudShellFullAccess

說明：與所有功能 AWS CloudShell 搭配使用的授權

AWSCloudShellFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudShellFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十五日, 世界標準時間 18:07
- 編輯時間:2020 年十二月十五日, 世界標準時間 18:07
- ARN: arn:aws:iam::aws:policy/AWSCloudShellFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudTrail_FullAccess

描述：提供對的完整存取權 AWS CloudTrail。

AWSCloudTrail_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudTrail_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 10 月 8 日, 23:41 世界標準時間
- 編輯時間：2021 年 2 月 22 日，世界標準時間 19:01
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudTrail_ReadOnlyAccess

描述：提供的唯讀存取權 AWS CloudTrail。

AWSCloudTrail_ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCloudTrail_ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 6 月 14 日，2022 年 17 月 19 日
- 編輯時間：世界標準時間 2022 年 6 月 14 日下午 17 時 19 分
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

描述：名為 AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents的服務連結角色會使用此原則。 CloudWatch 當 CloudWatch 警示進入 ALARM 狀態時，會使用此服務連結角色來執行 AWS 系統管理員事件管理員動作。此政策授予代表您啟動事件的權限。

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 4 月 27 日, 世界標準時間 13:30
- 編輯時間:2021 年 4 月 27 日, 世界標準時間 13:30
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeArtifactAdminAccess

描述：提供 AWS CodeArtifact 透過的完整存取 AWS Management Console。

AWSCodeArtifactAdminAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeArtifactAdminAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 16 日, 世界標準時間 23:53
- 編輯時間：2020 年 6 月 16 日，世界標準時間 23:53
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeArtifactReadOnlyAccess

描述：提供 AWS CodeArtifact 透過的唯讀存取 AWS Management Console。

AWSCodeArtifactReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeArtifactReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 25 日, 世界標準時間 21:23
- 編輯時間:2020 年 6 月 25 日, 世界標準時間 21:23
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeBuildAdminAccess

描述：提供 AWS CodeBuild 透過的完整存取 AWS Management Console。同時附加 AmazonS3 ReadOnlyAccess 以提供下載組建成品的存取權，並附加 IAM FullAccess 以建立和管理的服務角色。CodeBuild

`AWSCodeBuildAdminAccess`是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeBuildAdminAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年十二月一日, 19:04 世界標準時
- 編輯時間:2024 年 5 月 2 日, 01:45 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeBuildDeveloperAccess

描述：提供 AWS CodeBuild 透過的存取權 AWS Management Console，但不允許 CodeBuild 專案管理。還附加亞馬遜 S3 ReadOnlyAccess 以提供下載構建工件的訪問權限。

AWSCodeBuildDeveloperAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeBuildDeveloperAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年十二月 1 日, 世界標準時間 19:
- 編輯時間:2024 年 5 月 2 日, 01:36 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess

政策版本

策略版本：v15(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeBuildReadOnlyAccess

描述：提供 AWS CodeBuild 透過的唯讀存取 AWS Management Console。還附加亞馬遜 S3 ReadOnlyAccess 以提供下載構建工件的訪問權限。

AWSCodeBuildReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeBuildReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年十二月一日, 19:03 世界標準時
- 編輯時間:2024 年 5 月 2 日, 01:23 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

政策版本

策略版本：v12(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeCommitFullAccess

描述：提供 AWS CodeCommit 透過的完整存取 AWS Management Console。

AWSCodeCommitFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeCommitFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 7 月 9 日, 17:02 世界標準時間
- 編輯時間：世界標準時間 2023 年 7 月 17 日 21:50
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitFullAccess

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeCommitPowerUser

描述：提供儲存區域的完整 AWS CodeCommit 存取權，但不允許刪除儲存區域。

AWSCodeCommitPowerUser是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeCommitPowerUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 7 月 9 日, 2015 年 17 月 6 日
- 編輯時間：世界標準時間 2023 年 7 月 17 日 21:49
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitPowerUser

政策版本

策略版本：v15(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeCommitReadOnly

描述：提供 AWS CodeCommit 透過的唯讀存取 AWS Management Console。

`AWSCodeCommitReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`AWSCodeCommitReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 7 月 9 日, 17:05 世界標準時間

- 編輯時間:2021 年 8 月 18 日, 世界標準時間 18:18
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployDeployerAccess

描述：提供註冊和部署修訂的存取權。

AWSCodeDeployDeployerAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployDeployerAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 5 月 19 日, 18:18 世界標準時間
- 編輯時間：2020 年 4 月 2 日，世界標準時間 16:16
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployFullAccess

描述：提供對 CodeDeploy 資源的完整存取權。

AWSCodeDeployFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 5 月 19 日, 18:13 世界標準時間
- 編輯時間：2020 年 4 月 2 日，世界標準時間 16:14
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployReadOnlyAccess

描述：提供 CodeDeploy 資源的唯讀存取權。

AWSCodeDeployReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**:2015 年 5 月 19 日, 18:21 世界標準時間
- **編輯時間**：2020 年 4 月 2 日，世界標準時間 16:20
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployRole

描述：提供 CodeDeploy 服務存取權以展開標籤，並代表您與 Auto Scaling 互動。

AWSCodeDeployRole是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 5 月 4 日, 18:05 世界標準時間
- 編輯時間：世界標準時間 2023 年 8 月 16 日晚上 20:38
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployRoleForCloudFormation

描述：提供 CodeDeploy 服務存取權，以代表您叫用 Lambda 函數，以透過 CloudFormation執行藍/綠部署。

AWSCodeDeployRoleForCloudFormation是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployRoleForCloudFormation至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 5 月 19 日, 世界標準時間 17:12
- 編輯時間:2020 年 5 月 19 日, 世界標準時間 17:12
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployRoleForECS

描述：提供全 CodeDeploy 服務存取權，以代表您執行 ECS 藍/綠部署。授予支援服務的完整存取權，例如讀取所有 S3 物件的完整存取權、叫用所有 Lambda 函數、發佈到帳戶內的所有 SNS 主題，以及更新所有 ECS 服務。

AWSCodeDeployRoleForECS是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployRoleForECS至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十七日, 世界標準時間 20:40
- 編輯時間：2019 年 9 月 23 日，世界標準時間 22:37
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployRoleForECSLimited

描述：提供 CodeDeploy 服務有限的存取權，以代表您執行 ECS 藍/綠部署。

AWSCodeDeployRoleForECSLimited是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployRoleForECSLimited至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**2018 年十一月二十七日, 世界標準時間 20:42
- **編輯時間**：2019 年 9 月 23 日，世界標準時間 22:10
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployRoleForLambda

說明：提供 CodeDeploy 服務存取權，以代表您執行 Lambda 部署。

AWSCodeDeployRoleForLambda是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployRoleForLambda至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2017 年十一月二十八日，世界標準時間 14:05
- 編輯時間：2019 年 12 月 3 日，世界標準時間 19:53
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeDeployRoleForLambdaLimited

描述：提供 CodeDeploy 服務有限的存取權，以代表您執行 Lambda 部署。

AWSCodeDeployRoleForLambdaLimited是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeDeployRoleForLambdaLimited至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 8 月 17 日, 世界標準時間 17:14
- 編輯時間:2020 年 8 月 17 日, 世界標準時間 17:14
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodePipeline_FullAccess

描述：提供 AWS CodePipeline 透過的完整存取 AWS Management Console。

AWSCodePipeline_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodePipeline_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 3 日, 世界標準時間 22:38
- 編輯時間：世界標準時間 2024 年 3 月 14 日下午 17 時 6 分
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodePipeline_ReadOnlyAccess

描述：提供 AWS CodePipeline 透過的唯讀存取 AWS Management Console。

AWSCodePipeline_ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodePipeline_ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 3 日, 世界標準時間 22:25

- 編輯時間:2020 年 8 月 3 日, 世界標準時間 22:25
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodePipelineApproverAccess

描述：提供檢視和核准所有管道手動變更的存取權

AWSCodePipelineApproverAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodePipelineApproverAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2016 年 7 月 28 日, 世界標準時間 18:59
- 編輯時間:2017 年 8 月 2 日, 世界標準時間 17:24
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodePipelineCustomActionAccess

描述：提供自訂動作的存取權，以輪詢工作詳細資料 (包括臨時認證)，並將狀態更新報告給 AWS CodePipeline。

AWSCodePipelineCustomActionAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodePipelineCustomActionAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 7 月 9 日, 17:02 世界標準時間
- 編輯時間:2015 年 7 月 9 日, 世界標準時間 17:02
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeStarFullAccess

描述：提供 AWS CodeStar 透過的完整存取 AWS Management Console。

AWSCodeStarFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeStarFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 4 月 19 日, 世界標準時間 16:23
- 編輯時間：世界標準時間 2023 年 3 月 28 日凌時 06 分
- ARN: arn:aws:iam::aws:policy/AWSCodeStarFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeStarNotificationsServiceRolePolicy

說明：允許代表您存取 Amazon CloudWatch 事件的 AWS CodeStar 通知

`AWSCodeStarNotificationsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月五日, 16:10 世界標準時
- 編輯時間：2020 年 3 月 19 日，世界標準時間 16:01
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCodeStarServiceRole

說明：請勿使用-授與管理權限的 AWS CodeStar 服務角色政策， CodeStar 以便代表客戶管理 IAM 和其他服務資源。

AWSCodeStarServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AWSCodeStarServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 4 月 19 日, 世界標準時間 15:20
- 編輯時間：2021 年 9 月 20 日，世界標準時間 19:11
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCompromisedKeyQuarantine

說明：拒絕存取某些動作，這些動作由 AWS 團隊在 IAM 使用者的登入資料遭到入侵或公開時套用。請勿移除此原則。相反，請按照發送給您的有關此事件的電子郵件中指定的說明進行操作。

AWSCompromisedKeyQuarantine是AWS 受管理的策略。

使用此政策

您可以附加AWSCompromisedKeyQuarantine至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 11 日, 世界標準時間 18:04
- 編輯時間:2020 年 8 月 11 日, 世界標準時間 18:04
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCompromisedKeyQuarantineV2

說明：拒絕存取某些動作，這些動作由 AWS 團隊在 IAM 使用者的登入資料遭到入侵或公開時套用。請勿移除此原則。相反，請按照為您創建的有關此事件的支持案例中指定的說明進行操作。

AWSCompromisedKeyQuarantineV2是AWS 受管理的策略。

使用此政策

您可以附加AWSCompromisedKeyQuarantineV2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 4 月 21 日, 世界標準時間 22:30
- 編輯時間：世界標準時間 2023 年 3 月 16 日凌晨 12 時 20 分
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSConfigMultiAccountSetupPolicy

描述：允許 Config 在整個組織中呼叫 AWS 服務並部署設定資源

`AWSConfigMultiAccountSetupPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 6 月 17 日, 世界標準時間 18:03
- 編輯時間:2023 年 2 月 24 日, 01:39 世界標準時間
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSConfigRemediationServiceRolePolicy

描述：允許 AWS Config 代表您修復不符合標準的資源。

AWSConfigRemediationServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 6 月 18 日, 世界標準時間 21:21
- 編輯時間：2019 年 6 月 18 日，世界標準時間 21:21
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSConfigRoleForOrganizations

描述：允許組 AWS Config 呼叫唯讀 Or AWS ganizations API

AWSConfigRoleForOrganizations是AWS 受管理的策略。

使用此政策

您可以附加AWSConfigRoleForOrganizations至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 3 月 19 日, 世界標準時間 22:53
- 編輯時間：2020 年十一月二十四日，世界標準時間 20:19
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSConfigRulesExecutionRole

說明：允許 AWS Lambda 函數存取組態 API 和組態快照，以及設定定期交付給 Amazon S3 的組態快照。 AWS AWS 評估自訂 Config 規則之組態變更的函數需要此存取權。

AWSConfigRulesExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AWSConfigRulesExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一六年三月二十五日, 下午 17 點 59 分
- 編輯時間：2019 年 5 月 13 日，世界標準時間 21:33
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSConfigServiceRolePolicy

描述：允許 Config 代表您呼叫 AWS 服務並收集資源組態。

AWSConfigServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 5 月 30 日, 世界標準時間 23:31
- 編輯時間：世界標準時間 2024 年 2 月 22 日 17:20
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

政策版本

策略版本：v50(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
```

```
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
```

```
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
```

```
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
```

```
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
```

```
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
        "connect:DescribeRule",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
```

```
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
```

```
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
```

```
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
```

```
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
```

```
        "emr-serverless:ListApplications",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
```

```
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
```

```
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
```

```
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
```

```
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
```

```
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
```

```
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetFuotaTask",
```

```
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
```

```
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
```

```
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListCustomDataIdentifiers",
```

```
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListFlows",
        "mediaconnect:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
```

```
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
```

```
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
```

```
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "rekognition:DescribeStreamProcessor",
```

```
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
```

```
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
```

```
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
```

```
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListTags",
        "sagemaker:ListWorkteams",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
```

```
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
```

```
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
```

```
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
```

```
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSConfigUserAccess

描述：提供使用 AWS Config 的存取權，包括按資源上的標籤進行搜尋，以及讀取所有標籤。這不會提供設定 AWS Config 的權限，因為這需要系統管理權限。

AWSConfigUserAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSConfigUserAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一五年二月十八日, 19:38 世界標準時
- 編輯時間：2019 年 3 月 18 日，世界標準時間 20:27
- ARN: arn:aws:iam::aws:policy/AWSConfigUserAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSConnector

說明：允許對所有 EC2 物件進行廣泛的讀取/寫入存取、以 'import-to-ec2-' 開始對 S3 儲存貯體的讀取/寫入存取，以及列出所有 S3 儲存貯體的功能，讓 AWS 連接器代表您匯入 VM。

AWSConnector是AWS 受管理的策略。

使用此政策

您可以附加AWSConnector至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2015 年 2 月 11 日, 17:14
- 編輯時間：2015 年 9 月 28 日，世界標準時間 19:50
- ARN: arn:aws:iam::aws:policy/AWSConnector

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::import-to-ec2-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelConversionTask",
        "ec2:CancelExportTask",
        "ec2:CreateImage",
```

```
        "ec2:CreateInstanceExportTask",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:DetachVolume",
        "ec2:ImportInstance",
        "ec2:ImportVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CancelImportTask",
        "ec2:ImportSnapshot",
        "ec2:DescribeImportSnapshotTasks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSControlTowerAccountServiceRolePolicy

說明：允許 AWS Control Tower 呼叫提供自動化帳戶設定和集中式控管的 AWS 服務代表您。

AWSControlTowerAccountServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2023 年 6 月 5 日, 世界標準時間 22:04
- 編輯時間:世界標準時間 2023 年 6 月 5 日, 22:04
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSControlTowerServiceRolePolicy

描述：可存取 AWS Control Tower 管理或使用的 AWS 資源

AWSControlTowerServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSControlTowerServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2019 年 5 月 3 日, 18:19 世界標準時間

- 編輯時間:2023 年 4 月 12 日, 世界標準時間 19:15
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSCostAndUsageReportAutomationPolicy

描述：授與權限以描述帳戶組織、為 MAP 程式建立 S3 儲存貯體並套用標籤、建立成本和用量報告，以及描述成本和用量報告定義。

AWSCostAndUsageReportAutomationPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSCostAndUsageReportAutomationPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年 11 月 1 日, 世界標準時間 21:27
- 編輯時間:2021 年 11 月 1 日, 世界標準時間 21:27
- ARN: arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataExchangeFullAccess

描述：授與 AWS Data Exchange 的完整存取權限，以及使用 AWS Management Console 和 SDK 的 AWS Marketplace 動作。它還提供了對充分利用 AWS Data Exchange 所需的相關服務的選擇訪問權限。

AWSDataExchangeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDataExchangeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月十三日, 世界標準時間
- 編輯時間:世界標準時間 5 月 7 日, 下午 17 時 4 分
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeFullAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataExchangeProviderFullAccess

描述：授予資料提供者對 AWS Data Exchange 的存取權限，以及使用 AWS Management Console 和 SDK 的 AWS Marketplace 動作。它還提供了對充分利用 AWS Data Exchange 所需的相關服務的選擇訪問權限。

AWSDataExchangeProviderFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDataExchangeProviderFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月十三日, 世界標準時間
- 編輯時間：世界標準時間 2022 年 3 月 15 日，16:16
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataExchangeReadOnly

描述：授與 AWS Data Exchange 的唯讀存取權限，以及使用 AWS Management Console 和 SDK 的 AWS Marketplace 動作。

AWSDataExchangeReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSDataExchangeReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**二零一九年十一月十三日, 世界標準時間
- **編輯時間:**2021 年 5 月 10 日, 世界標準時間 21:15
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataExchangeSubscriberFullAccess

說明：授與資料訂閱者存取 AWS Data Exchange，以及使用 AWS Management Console 和 SDK 的 AWS Marketplace 動作。它還提供了對充分利用 AWS Data Exchange 所需的相關服務的選擇訪問權限。

`AWSDataExchangeSubscriberFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSDataExchangeSubscriberFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月十三日, 世界標準時間
- 編輯時間：世界標準時間 11 月 29 日晚上 11 點
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataLifecycleManagerServiceRole

描述：提供適當的權限給資 AWS 料生命週期管理員，以對 AWS 資源採取動作

AWSDataLifecycleManagerServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AWSDataLifecycleManagerServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 7 月 6 日, 世界標準時間 19:34
- 編輯時間：2022 年 9 月 19 日，世界標準時間 17：34
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataLifecycleManagerServiceRoleForAMIManagement

描述：提供適當的權限給資 AWS 料生命週期管理員，以針對 AMI 管理的 AWS 資源採取動作

`AWSDataLifecycleManagerServiceRoleForAMIManagement`是AWS 受管理的策略。

使用此政策

您可以附加`AWSDataLifecycleManagerServiceRoleForAMIManagement`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年十月 21 日, 世界標準時間 19:39
- 編輯時間:2021 年 8 月 19 日, 世界標準時間 17:03
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataLifecycleManagerSSMFullAccess

說明：提供 Amazon Data Lifecycle Manager 許可，以執行在所有 Amazon EC2 執行個體上執行指令碼前後執行所需的 Systems Manager 動作。

AWSDataLifecycleManagerSSMFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDataLifecycleManagerSSMFullAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2023 年 10 月 31 日, 世界標準時間 20:29
- 編輯時間：世界標準時間 2023 年 11 月 16 日晚上 22 時 31 分
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataPipeline_FullAccess

描述：提供對 Data Pipeline 的完整存取權、清單 S3、DynamoDB、Redshift、RDS、SNS 和 IAM 角色的存取權限，以及預設角色的密碼角色存取權。

AWSDataPipeline_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDataPipeline_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 19 日, 世界標準時間 23:14
- 編輯時間：2017 年 8 月 17 日，世界標準時間 18:48
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataPipeline_PowerUser

描述：提供對 Data Pipeline 的完整存取權、清單 S3、DynamoDB、Redshift、RDS、SNS 和 IAM 角色的存取權限，以及預設角色的密碼角色存取權。

AWSDataPipeline_PowerUser是AWS 受管理的策略。

使用此政策

您可以附加AWSDataPipeline_PowerUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 19 日, 世界標準時間 23:16
- 編輯時間：2017 年 8 月 17 日，世界標準時間 18:49
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataSyncDiscoveryServiceRolePolicy

描述：允許 DataSync 探索代表您與其他 AWS 服務整合。

AWSDataSyncDiscoveryServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2023 年 3 月 20 日, 22:19
- 編輯時間:世界標準時間 2023 年 3 月 20 日, 22:19
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataSyncFullAccess

描述：提供對其相依性的完整存取權 AWS DataSync 和最小存取權

`AWSDataSyncFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSDataSyncFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**:2019 年 1 月 18 日, 世界標準時間 19:40
- **編輯時間**：世界標準時間 2024 年 2 月 16 日下午 17 時 19 分
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDataSyncReadOnlyAccess

描述：提供唯讀存取權 AWS DataSync

AWSDataSyncReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDataSyncReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 1 月 18 日, 世界標準時間 19:18
- 編輯時間:2020 年 6 月 30 日, 世界標準時間 17:59
- ARN: arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeadlineCloud-FleetWorker

描述：提供 AWS 期限雲端工作者存取在伺服器陣列上執行工作的權限。

AWSDeadlineCloud-FleetWorker是AWS 受管理的策略。

使用此政策

您可以附加AWSDeadlineCloud-FleetWorker至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 4 月 1 日, 下午 17 時 21 分
- 編輯時間：世界標準時間 2024 年 4 月 1 日 17:21
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeadlineCloud-UserAccessFarms

描述：提供使用者工作站存取 AWS 期限雲端伺服器陣列的有限唯讀權限，以呼叫其他必要的服務。將此策略附加到與您的工作室相關聯的用戶角色。

AWSDeadlineCloud-UserAccessFarms是AWS 受管理的策略。

使用此政策

您可以附加AWSDeadlineCloud-UserAccessFarms至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2024 年 4 月 1 日, 16:54 世界標準時間
- 編輯時間：世界標準時間 2024 年 4 月 1 日，16:54
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeadlineCloud-UserAccessFleets

描述：提供使用者工作站以有限的唯讀權限存取 AWS 截止日期雲端叢集，以呼叫其他必要的服務。將此策略附加到與您的工作室相關聯的用戶角色。

AWSDeadlineCloud-UserAccessFleets是AWS 受管理的策略。

使用此政策

您可以附加AWSDeadlineCloud-UserAccessFleets至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 1 日, 世界標準時間 17:01
- 編輯時間：世界標準時間 2024 年 4 月 1 日 17:01
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeadlineCloud-UserAccessJobs

描述：提供使用者工作站以有限的唯讀權限存取 AWS 截止日期 Cloud 工作，以呼叫其他必要的服務。將此原則附加到與您的工作室相關聯的使用者角色。

AWSDeadlineCloud-UserAccessJobs是AWS 受管理的策略。

使用此政策

您可以附加AWSDeadlineCloud-UserAccessJobs至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 1 日, 世界標準時間 17:05
- 編輯時間：世界標準時間 2024 年 4 月 1 日下午 17 時 05 分
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeadlineCloud-UserAccessQueues

描述：提供使用者工作站以有限的唯讀權限存取 AWS 截止日期雲端佇列，以呼叫其他必要的服務。將此策略附加到與您的工作室相關聯的用戶角色。

AWSDeadlineCloud-UserAccessQueues是AWS 受管理的策略。

使用此政策

您可以附加AWSDeadlineCloud-UserAccessQueues至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 4 月 1 日, 下午 17 點 10 分
- 編輯時間：世界標準時間 2024 年 4 月 1 日 17:10
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeadlineCloud-WorkerHost

描述：提供 AWS 期限雲端工作者主機加入伺服器陣列中叢集的存取權。

AWSDeadlineCloud-WorkerHost是AWS 受管理的策略。

使用此政策

您可以附加AWSDeadlineCloud-WorkerHost至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 1 日, 世界標準時間 17:28
- 編輯時間：世界標準時間 2024 年 4 月 1 日 17:28
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeepLensLambdaFunctionAccessPolicy

描述：此原則指定在 DeepLens 裝置上執行的 DeepLens 管理 lambda 函數所需的權限

AWSDeepLensLambdaFunctionAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSDeepLensLambdaFunctionAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 11 月 29 日，世界標準時間 15:47
- 編輯時間：2019 年 6 月 11 日，世界標準時間 23:11
- ARN: arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeepLensServiceRolePolicy

說明：授予 AWS DeepLens 存取權限 AWS 服務、資源和角色，以 DeepLens 及其相依性 (包括 IoT、S3 和 AWS Lambda) 所需的資源 GreenGrass 和角色。

AWSDeepLensServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSDeepLensServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2017 年 11 月 29 日，世界標準時間 15:46
- 編輯時間：2019 年 9 月 25 日，世界標準時間 19:25
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeepRacerAccountAdminAccess

描述： DeepRacer 管理員存取所有動作，包括在多使用者和單一使用者模式之間切換。

AWSDeepRacerAccountAdminAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDeepRacerAccountAdminAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二一年十月二十八日, 01:27 世界時間
- 編輯時間:二零二一年十月二十八日, 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeepRacerCloudFormationAccessPolicy

描述： CloudFormation 允許代表您創建和管理 AWS 堆棧和資源。

AWSDeepRacerCloudFormationAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSDeepRacerCloudFormationAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年二月 28 日, 世界標準時間 21:59
- 編輯時間：2019 年 6 月 14 日, 世界標準時間 17:02
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeepRacerDefaultMultiUserAccess

描述：在多重使用者模式下使用 deepracer 的 DeepRacer MultiUser 預設使用者存取權

AWSDeepRacerDefaultMultiUserAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDeepRacerDefaultMultiUserAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二一年十月二十八日, 01:27 世界時間
- 編輯時間:二零二一年十月二十八日, 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeepRacerFullAccess

描述：提供對的完整存取權 AWS DeepRacer。也提供對相關服務 (例如 S3) 的選取存取權。

AWSDeepRacerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDeepRacerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 10 月 5 日, 世界標準時間 22:03
- 編輯時間:2020 年 10 月 5 日, 世界標準時間 22:03
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeepRacerRoboMakerAccessPolicy

描述： RoboMaker 允許創建所需的資源並代表您調用 AWS 服務。

AWSDeepRacerRoboMakerAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSDeepRacerRoboMakerAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年二月 28 日, 世界標準時間 21:59
- 編輯時間：2019 年 2 月 28 日，世界標準時間 21:59
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeepRacerServiceRolePolicy

描述： DeepRacer 允許創建所需的資源並代表您調用 AWS 服務。

AWSDeepRacerServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSDeepRacerServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一九年二月二十八日, 21:58 世界標準
- 編輯時間：2019 年 6 月 12 日，世界標準時間 20:55
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDenyAll

描述：拒絕所有存取。

AWSDenyAll是AWS 受管理的策略。

使用此政策

您可以附加AWSDenyAll至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 5 月 1 日, 世界標準時間 22:36
- 編輯時間：世界標準時間 2023 年十二月十八日 16:42
- ARN: arn:aws:iam::aws:policy/AWSDenyAll

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeviceFarmFullAccess

描述：提供所有 AWS Device Farm 作業的完整存取權。

AWSDeviceFarmFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDeviceFarmFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- 創建時間:2015 年 7 月 13 日, 16:37 世界標準時間
- 編輯時間：2015 年 7 月 13 日，世界標準時間 16:37
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeviceFarmServiceRolePolicy

說明：授與權限給 AWS Device Farm，以代表您呼叫 EC2 網路 API。

`AWSDeviceFarmServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間（世界標準時間）9 月 20 日
- 編輯時間：世界標準時間 2022 年 9 月 20 日晚上 9 時 02 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDeviceFarmTestGridServiceRolePolicy

說明：授與權限給 AWS Device Farm，以代表您呼叫 EC2 API。

AWSDeviceFarmTestGridServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 5 月 26 日, 世界標準時間 22:01
- 編輯時間：2021 年 5 月 26 日，世界標準時間 22 點 1
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDirectConnectFullAccess

描述：提供透過「 AWS 直接 Connect」的完整存取權 AWS Management Console。

`AWSDirectConnectFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSDirectConnectFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2019 年 4 月 30 日，世界標準時間 15:29

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

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDirectConnectReadOnlyAccess

說明：透過提供 AWS 直接 Connect 的唯讀存取權 AWS Management Console。

`AWSDirectConnectReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加AWSDirectConnectReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間:2020 年 5 月 18 日, 世界標準時間 18:48
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDirectConnectServiceRolePolicy

描述：提供「AWS 直 Connect」權限，以代表您建立和管理 AWS 資源。

AWSDirectConnectServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 1 月 14 日, 世界標準時間 18:35
- 編輯時間:2021 年 1 月 14 日, 世界標準時間 18:35
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

```
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDirectoryServiceFullAccess

描述：提供「 AWS Directory Service」的完整存取權。

`AWSDirectoryServiceFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSDirectoryServiceFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間:2024 年 4 月 2 日, 世界標準時間 20:38
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDirectoryServiceReadOnlyAccess

描述：提供「 AWS Directory Service」的唯讀存取權。

AWSDirectoryServiceReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSDirectoryServiceReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2018 年 9 月 25 日，世界標準時間 21:54
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDiscoveryContinuousExportFirehosePolicy

描述：提供「AWS 探索連續匯出」所需 AWS 資源的寫入存取權

AWSDiscoveryContinuousExportFirehosePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSDiscoveryContinuousExportFirehosePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 8 月 9 日, 18:29 世界標準時間
- 編輯時間：2021 年 6 月 8 日，世界標準時間 17：32
- ARN: arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDMSFleetAdvisorServiceRolePolicy

描述：允許 DMS 叢集建議程式代表您管理 CloudWatch 指標。

`AWSDMSFleetAdvisorServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 3 月 6 日，09:10
- 編輯時間：世界標準時間 2023 年 3 月 6 日 09:10
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSDMSServerlessServiceRolePolicy

說明：授予 AWS DMS 無伺服器權限，以代表您在帳戶中建立及管理 DMS 資源

AWSDMSServerlessServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2023 年 5 月 18 日, 世界標準時間 20:28
- 編輯時間:2023 年 5 月 18 日, 世界標準時間 20:28
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSEC2CapacityReservationFleetRolePolicy

說明：允許 EC2 CapacityReservation 叢集服務管理容量保留

AWSEC2CapacityReservationFleetRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2021 年 9 月 29 日，世界標準時間 14:43
- 編輯時間：2021 年 9 月 29 日，世界標準時間 14:43
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSEC2FleetServiceRolePolicy

說明：允許 EC2 叢集啟動和管理執行個體。

AWSEC2FleetServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2018 年 3 月 21 日，世界標準時間 00:08

- 編輯時間:2020 年 5 月 4 日, 世界標準時間 20:10
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSEC2SpotFleetServiceRolePolicy

說明：允許 EC2 Spot 叢集啟動和管理競價型叢集執行個體

AWSEC2SpotFleetServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 10 月 23 日, 世界標準時間 19:13
- 編輯時間：2020 年 3 月 16 日，世界標準時間 19:16
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSEC2SpotServiceRolePolicy

說明：允許 EC2 Spot 啟動和管理競價型執行個體

AWSEC2SpotServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 9 月 18 日, 世界標準時間 18:51
- 編輯時間:2018 年十二月十二日, 00:13 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSEC2VssSnapshotPolicy

說明：此政策附加到附加到 Amazon EC2 Windows 執行個體的 IAM 角色，以使 Amazon EC2 VSS 解決方案能夠建立和新增標籤至 Amazon 機器映像 (AMI) 和 EBS 快照。

AWSEC2VssSnapshotPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSEC2VssSnapshotPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2024 年 3 月 27 日，16:32
- 編輯時間：世界標準時間 2024 年 3 月 27 日下午 16:32
- ARN: arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSECRPullThroughCache_ServiceRolePolicy

描述：允許存取 AWS ECR 透過快取提取所使用或管理的 AWS 服務和資源

AWSECRPullThroughCache_ServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年十一月二十六日, 世界標準時間 21:51
- 編輯時間：世界標準時間 2023 年 11 月 13 日，下午 3:23
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkCustomPlatformforEC2Role

說明：提供自訂平台建置器環境中的執行個體許可，以啟動 EC2 執行個體、建立 EBS 快照和 AMI、將日誌串流到 Amazon CloudWatch 日誌，以及在 Amazon S3 中存放成品。

AWSElasticBeanstalkCustomPlatformforEC2Role是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkCustomPlatformforEC2Role至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 2 月 21 日, 世界標準時間 22:50
- 編輯時間：2017 年 2 月 21 日，世界標準時間 22:50
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkEnhancedHealth

說明：Health 監測系統的 E AWS lastic Beanstalk 服務政策

`AWSElasticBeanstalkEnhancedHealth`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticBeanstalkEnhancedHealth`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：二零一六年二月八日 23:17 世界標準時間
- 編輯時間:2018 年 4 月 9 日, 世界標準時間 22:12
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkMaintenance

描述：E AWS lastic Beanstalk 服務角色政策，授予有限權限，以代表您更新資源以進行維護。

`AWSElasticBeanstalkMaintenance`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 1 月 11 日, 世界標準時間 23:22
- 編輯時間：世界標準時間 2024 年 4 月 29 日 21:48
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

描述：此原則適用於 E AWS lastic Beanstalk 服務角色，用來執行 Elastic Beanstalk 環境的管理更新。此原則不應附加至其他使用者或角色。該政策授予跨多種 AWS 服務建立和管理資源的廣泛許可

AutoScaling，包括 EC2、ECS、Elastic Load Balancing 和 CloudFormation. 此政策還允許傳遞可用於這些服務的任何 IAM 角色。

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2021 年 3 月 3 日, 22:18
- 編輯時間：世界標準時間 2023 年 3 月 23 日 23:15
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcs",
```

```
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2BroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteSecurityGroup",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2RunInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
```

```
      }
    },
    {
      "Sid" : "EC2TerminateInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "ECSBroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSDeleteClusterOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ecs:DeleteCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Sid" : "ASGOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
```

```
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFNOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "ELBOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
```

```
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*"
      ]
    },
    {
      "Sid" : "CWLogsOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "S3ObjectOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3BucketOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
```

```
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "SNSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Sid" : "SQSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Sid" : "CWPutMetricAlarmOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

描述：可授與受管理更新的有限權限的 E AWS lastic Beanstalk 服務角色政策。

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月二十一日, 世界標準時
- 編輯時間：世界標準時間 2024 年 4 月 29 日 23:11
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkMulticontainerDocker

說明：提供多容器 Docker 環境中的執行個體存取權，以使用 Amazon EC2 Container Service 來管理容器部署任務。

`AWSElasticBeanstalkMulticontainerDocker`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticBeanstalkMulticontainerDocker`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2016 年 2 月 8 日, 23:15 世界標準時間
- 編輯時間:世界標準時間 2023 年 3 月 23 日, 22:04

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

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkReadOnly

描述：授與唯讀權限。明確允許運營商直接訪問，以檢索與 E AWS lastic Beanstalk 應用程序相關的資源的信息。

AWSElasticBeanstalkReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 1 月 22 日, 世界標準時間 19:02
- 編輯時間：2021 年 1 月 22 日，世界標準時間 19:02
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkRoleCore

描述： AWSElasticBeanstalkRoleCore (Elastic Beanstalk 作業角色) 允許 Web 服務環境的核心作業。

AWSElasticBeanstalkRoleCore是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkRoleCore至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 6 月 5 日, 世界標準時間 21:48
- 編輯時間：世界標準時間 2024 年 4 月 30 日凌時 01 分
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*/*",
        "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
      ]
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:ContinueUpdateRollback",
```

```
        "cloudformation:CancelUpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing:Delete*",
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
      ]
    },
    {
      "Sid" : "ListAPIs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "logs:Describe*",
        "ec2:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticloadbalancing:Describe*",
        "rds:Describe*",
        "sns:List*",
        "iam:List*",
        "acm:Describe*",
        "acm:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkRoleCWL

描述：(Elastic Beanstalk 操作角色) 允許環境管理 Amazon CloudWatch 日誌記錄群組。

AWSElasticBeanstalkRoleCWL是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkRoleCWL至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 6 月 5 日, 21:49 世界標準時間
- 編輯時間：2020 年 6 月 5 日，世界標準時間 21:49
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
```

```
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkRoleECS

描述：(Elastic Beanstalk 作業角色) 允許多容器泊塢視窗環境管理 Amazon ECS 叢集。

AWSElasticBeanstalkRoleECS是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkRoleECS至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 6 月 5 日, 世界標準時間 21:47
- 編輯時間:世界標準時間 2023 年 3 月 23 日, 22:43
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkRoleRDS

說明：(Elastic Beanstalk 操作角色) 允許環境整合 Amazon RDS 執行個體。

AWSElasticBeanstalkRoleRDS是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkRoleRDS至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 6 月 5 日, 世界標準時間 21:46
- 編輯時間：2020 年 6 月 5 日，世界標準時間 21:46
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkRoleSNS

描述：(Elastic Beanstalk 操作角色) 允許環境啟用 Amazon SNS 主題整合。

AWSElasticBeanstalkRoleSNS是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkRoleSNS至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 6 月 5 日, 世界標準時間 21:46
- 編輯時間：2020 年 6 月 5 日，世界標準時間 21:46
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkRoleWorkerTier

說明：(Elastic Beanstalk 操作角色) 允許工作者環境層建立 Amazon DynamoDB 表格和 Amazon SQS 佇列。

AWSElasticBeanstalkRoleWorkerTier是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkRoleWorkerTier至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 6 月 5 日, 世界標準時間 21:43
- 編輯時間:2020 年 6 月 5 日, 世界標準時間 21:43
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkService

說明：此原則位於淘汰路徑上。請參閱說明文件以取得指引：https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html。 AWS Elastic Beanstalk 服務角色政策，授予代表您創建和管理資源（即 EC2 AutoScaling CloudFormation，S3，ELB 等）的許可。

`AWSElasticBeanstalkService`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticBeanstalkService`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2016 年 4 月 11 日, 世界標準時間 20:27

- 編輯時間:2023 年 5 月 10 日, 世界標準時間 19:29
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService

政策版本

策略版本：v17(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkServiceRolePolicy

說明：E AWS lastic Beanstalk 服務連結角色政策，授予代表您建立和管理資源 (即 EC2 AutoScaling CloudFormation、S3、ELB 等) 的權限。

`AWSElasticBeanstalkServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年 9 月 13 日，世界標準時間 23:46
- 編輯時間：2019 年 6 月 6 日，世界標準時間 21:59
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkWebTier

說明：提供 Web 伺服器環境中的執行個體存取權，以便將日誌檔上傳到 Amazon S3。

AWSElasticBeanstalkWebTier是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticBeanstalkWebTier至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一六年二月八日 23:08 世界標準時間
- 編輯時間：2020 年 9 月 9 日，世界標準時間 19:38
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticBeanstalkWorkerTier

描述：提供工作者環境中的執行個體存取權，以便將日誌檔上傳到 Amazon S3、使用 Amazon SQS 監控應用程式的任務佇列、使用 Amazon DynamoDB 執行領導者選舉，以及向 Amazon CloudWatch 發佈健康狀態監控指標。

`AWSElasticBeanstalkWorkerTier`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticBeanstalkWorkerTier`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一六年二月八日 23:12 世界標準時間
- 編輯時間：2020 年 9 月 9 日，世界標準時間 19:53
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryAgentInstallationPolicy

描述：此原則允許安裝 AWS 複寫代理程式，此代理程式可與 AWS 彈性災難復原 (DRS) 搭配使用，以將外部伺服器復原至 AWS。將此政策附加到您在 AWS 複寫代理程式安裝步驟期間提供其登入資料的 IAM 使用者或角色。

`AWSElasticDisasterRecoveryAgentInstallationPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticDisasterRecoveryAgentInstallationPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年十一月十七日, 世界標準時間 10:37
- 編輯時間：世界標準時間：2023 年 11 月 27 日上午 12:38
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryAgentPolicy

描述：此原則允許使用與 AWS 彈性災難復原 (DRS) 搭配使用的 AWS 複寫代理程式，將來源伺服器復原至 AWS。我們不建議您將此政策附加到 IAM 使用者或角色。

`AWSElasticDisasterRecoveryAgentPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticDisasterRecoveryAgentPolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略

- **創建時間**：2021 年十一月十七日，世界標準時間 10:32
- **編輯時間**：世界標準時間：2023 年 11 月 27 日，下午 13:44
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryConsoleFullAccess

說明：此政策提供對 AWS 彈性災難復原 (DRS) 的所有公用 API 的完整存取權，以及讀取 KMS 金鑰、License Manager、Resource Groups、Elastic Load Balancing、IAM 和 EC2 資訊的許可。將此政策附加到您的 IAM 使用者或角色。

`AWSElasticDisasterRecoveryConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticDisasterRecoveryConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月十七日，世界標準時間 10:46
- 編輯時間：世界標準時間 2023 年 10 月 16 日 12:24
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryConsoleFullAccess_v2

描述：此原則提供對 AWS 彈性災難復原 (AWS DRS) 的所有公用 API 的完整存取權，以及 DRS Console 所使用之其他 AWS 服務中的所有公用 API。 AWS 將此原則附加至您的使用者或角色。

AWSElasticDisasterRecoveryConsoleFullAccess_v2是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryConsoleFullAccess_v2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：2023 年 11 月 27 日，下午 13:35
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 13:35
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
```

```
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
```

```
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryConversionServerPolicy

描述：此原則會附加至 AWS 彈性災難復原轉換伺服器的執行個體角色。此原則允許彈性災難復原 (DRS) 轉換伺服器 (由彈性災難復原啟動的 EC2 執行個體) 與 DRS 服務通訊。DRS 會將具有此政策的 IAM 角色 (做為 EC2 執行個體設定檔) 附加至 DRS 轉換伺服器，並在需要時由 DRS 自動啟動和終止。我們不建議您將此政策附加到 IAM 使用者或角色。當使用者選擇使用 DRS 主控台、CLI 或 API 復原來源伺服器時，彈性災難復原會使用 DRS 轉換伺服器。

`AWSElasticDisasterRecoveryConversionServerPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticDisasterRecoveryConversionServerPolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年十一月十七日, 世界標準時間 13:42
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 13:13
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

描述：此原則允許 AWS 彈性災難復原 (DRS) 支援跨帳戶複寫和跨帳戶容錯回復。

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryCrossAccountReplicationPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 5 月 14 日，07:16
- 編輯時間:世界標準時間 2024 年 1 月 17 日, 13:19
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryEc2InstancePolicy

描述：此原則允許安裝和使用 AWS 彈性災難復原 (DRS) 所使用的 AWS 複寫代理程式，以復原 EC2 (跨區域或跨可用區域) 上執行的來源伺服器。應將具有此政策的 IAM 角色 (做為 EC2 執行個體設定檔) 附加至 EC2 執行個體。

AWSElasticDisasterRecoveryEc2InstancePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryEc2InstancePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2022 年 5 月 26 日, 世界標準時間中午 12 點 30

- **編輯時間**：世界標準時間：2023 年 11 月 27 日，下午 13:39
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryFailbackInstallationPolicy

說明：您可以將政 AWSElasticDisasterRecoveryFailbackInstallationPolicy 策附加到 IAM 身分。此原則允許安裝彈性災難復原容錯回復用戶端，用於將復原執行個體容錯回復至原始來源基礎結構。將此政策附加到您在執行彈性災難復原容錯回復用戶端時提供其登入資料的 IAM 使用者或角色。

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticDisasterRecoveryFailbackInstallationPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月十七日, 世界標準時間 11:02
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 13:43
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryFailbackPolicy

說明：此原則允許使用彈性災難復原容錯回復用戶端，用來將復原執行個體回復至原始來源基礎結構。我們不建議您將此政策附加到 IAM 使用者或角色。

AWSElasticDisasterRecoveryFailbackPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryFailbackPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2021 年十一月十七日, 世界標準時間 10:41
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 12:56
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryLaunchActionsPolicy

說明：此政策可讓您使用 Amazon SSM 和其他所需的服務許可，在 AWS 彈性災難復原 (AWS DRS) 中執行啟動後動作。將此政策附加到您的 IAM 角色或使用者。

`AWSElasticDisasterRecoveryLaunchActionsPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticDisasterRecoveryLaunchActionsPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 9 月 13 日 07:38
- 編輯時間：世界標準時間 2023 年 10 月 16 日 12:28
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/AWSDistroOTel-*",
        "arn:aws:ssm:*::document/AWSDocs-*",
        "arn:aws:ssm:*::document/AWSEC2-*",
        "arn:aws:ssm:*::document/AWSEC2Launch-*",
        "arn:aws:ssm:*::document/AWSFIS-*",
        "arn:aws:ssm:*::document/AWSFleetManager-*",
        "arn:aws:ssm:*::document/AWSIncidents-*",
        "arn:aws:ssm:*::document/AWSKinesisTap-*",
        "arn:aws:ssm:*::document/AWSMigration-*",
        "arn:aws:ssm:*::document/AWSNVMe-*",
        "arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
        "arn:aws:ssm:*::document/AWSObservabilityExporter-*",
        "arn:aws:ssm:*::document/AWSPVDriver-*",
        "arn:aws:ssm:*::document/AWSQuickSetupType-*",
        "arn:aws:ssm:*::document/AWSQuickStarts-*",
        "arn:aws:ssm:*::document/AWSRefactorSpaces-*",
        "arn:aws:ssm:*::document/AWSResilienceHub-*",
        "arn:aws:ssm:*::document/AWSSAP-*",
        "arn:aws:ssm:*::document/AWSSAPTools-*",
        "arn:aws:ssm:*::document/AWSSQLServer-*",
        "arn:aws:ssm:*::document/AWSSSO-*",
        "arn:aws:ssm:*::document/AWSSupport-*",
        "arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
        "arn:aws:ssm:*::document/AmazonCloudWatch-*",
        "arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
        "arn:aws:ssm:*::document/AmazonECS-*",
        "arn:aws:ssm:*::document/AmazonEFSUtils-*",
        "arn:aws:ssm:*::document/AmazonEKS-*",
        "arn:aws:ssm:*::document/AmazonInspector-*",
        "arn:aws:ssm:*::document/AmazonInspector2-*",
        "arn:aws:ssm:*::document/AmazonInternal-*",
        "arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
        "arn:aws:ssm:*::document/AwsVssComponents-*",
        "arn:aws:ssm:*::automation-definition/AWS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
```

```
        "arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "LaunchActionsPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy6",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchActionsPolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "LaunchActionsPolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "LaunchActionsPolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy11",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "drs.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryNetworkReplicationPolicy

描述：此原則允許 AWS 彈性災難復原 (DRS) 支援網路複寫。

AWSElasticDisasterRecoveryNetworkReplicationPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryNetworkReplicationPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 6 月 11 日，下午 12:36
- 編輯時間：世界標準時間 2024 年 1 月 2 日，13:25
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryReadOnlyAccess

說明：您可以將政 AWSElasticDisasterRecoveryReadOnlyAccess 策附加到 IAM 身分。此原則提供彈性災難復原 (DRS) 的所有唯讀公用 API 的權限，以及其他 AWS 服務的一些唯讀 API，才能完全唯讀使用 DRS 主控台。將此政策附加到您的 IAM 使用者或角色。

`AWSElasticDisasterRecoveryReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElasticDisasterRecoveryReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月十七日, 世界標準時間 10:50
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 13:03
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryRecoveryInstancePolicy

說明：此原則附加至彈性災難復原的復原執行個體的執行個體角色。此政策允許彈性災難復原 (DRS) 復原執行個體 (由彈性災難復原啟動的 EC2 執行個體) 與 DRS 服務通訊，並能夠容錯回復至其原始來源基礎架構。彈性災難復原會將具有此政策的 IAM 角色 (做為 EC2 執行個體設定檔) 附加至 DRS 復原執行個體。我們不建議您將此政策附加到 IAM 使用者或角色。

AWSElasticDisasterRecoveryRecoveryInstancePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryRecoveryInstancePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 11 月 17 日，上午 10:20
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 13:11
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryReplicationServerPolicy

描述：此原則會附加至彈性災難復原複寫伺服器的執行個體角色。此原則允許彈性災難復原 (DRS) 複寫伺服器 (由彈性災難復原啟動的 EC2 執行個體) 與 DRS 服務通訊，並在您的. AWS 帳戶彈性災難復原會將具有此政策的 IAM 角色 (做為 EC2 執行個體設定檔) 連接至 DRS 複寫伺服器，這些伺服器會根

據需要由 DRS 自動啟動和終止。DRS 複製伺服器可用來協助將資料從外部伺服器複製到 AWS，作為 DRS 管理的復原程序的一部分。我們不建議您將此政策附加到 IAM 使用者或角色。

AWSElasticDisasterRecoveryReplicationServerPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryReplicationServerPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2021 年十一月十七日，世界標準時間 13:34
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 13:28
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryServiceRolePolicy

描述：此原則允許彈性災難復原代表您管理 AWS 資源。

AWSElasticDisasterRecoveryServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2021 年十一月十七日，世界標準時間 10:56
- 編輯時間：世界標準時間 2024 年 1 月 17 日下午 13:49
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryStagingAccountPolicy

描述：此原則允許以唯讀方式存取 AWS 彈性災難復原 (DRS) 資源，例如來源伺服器和作業。它也允許建立轉換後的快照，並與特定帳戶共用該 EBS 快照。

AWSElasticDisasterRecoveryStagingAccountPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryStagingAccountPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：2022 年 5 月 26 日，09:49
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 13:07
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

描述： AWS 彈性災難復原 (DRS) 會使用此原則將來源伺服器復原至個別的目標帳戶，並允許失敗回復。我們不建議您將此政策附加到 IAM 使用者或角色。

AWSElasticDisasterRecoveryStagingAccountPolicy_v2是AWS 受管理的策略。

使用此政策

您可以附加AWSElasticDisasterRecoveryStagingAccountPolicy_v2至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 2023 年 1 月 5 日 12:11
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 13:32
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticLoadBalancingClassicServiceRolePolicy

說明：E AWS lastic Load Balancing 控制平面的服務連結角色原則-典型

AWSElasticLoadBalancingClassicServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年 9 月 19 日，世界標準時間 22:36
- 編輯時間：2019 年 10 月 7 日，世界標準時間 23:04
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElasticLoadBalancingServiceRolePolicy

說明：E AWS lastic Load Balancing 控制平面的服務連結角色原則

`AWSElasticLoadBalancingServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間**：2017 年 9 月 19 日，世界標準時間 22:19
- **編輯時間**：2021 年 8 月 26 日，世界標準時間 19:01
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaConvertFullAccess

描述： MediaConvert 透過 AWS Management Console 和 SDK 提供對 AWS 元素的完整存取權。

`AWSElementalMediaConvertFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElementalMediaConvertFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 25 日, 世界標準時間 19:25
- 編輯時間：2019 年 6 月 10 日，世界標準時間 22:52
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaConvertReadOnly

描述： MediaConvert 透過 AWS Management Console 和 SDK 提供 AWS 元素的唯讀存取權。

AWSElementalMediaConvertReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaConvertReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 25 日, 世界標準時間 19:25
- 編輯時間：2019 年 6 月 10 日，世界標準時間 22:52
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
```

```
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaLiveFullAccess

描述：提供對 AWS 元素 MediaLive 資源的完整存取

AWSElementalMediaLiveFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaLiveFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 7 月 8 日, 世界標準時間 17:07
- 編輯時間:2020 年 7 月 8 日, 世界標準時間 17:07
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaLiveReadOnly

描述：提供 AWS 元素 MediaLive 資源的唯讀存取權

AWSElementalMediaLiveReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaLiveReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 7 月 8 日, 世界標準時間 16:38
- 編輯時間：2020 年 7 月 8 日，世界標準時間 16:38
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaPackageFullAccess

描述：提供 AWS 元素 MediaPackage 資源的完整存取權

AWSElementalMediaPackageFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaPackageFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年十二月二十九日, 23:39 世界標準時間
- 編輯時間：2017 年十二月二十九日，世界標準時間 23:39
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaPackageReadOnly

描述：提供 AWS 元素 MediaPackage 資源的唯讀存取權

`AWSElementalMediaPackageReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaPackageReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十二月三十日，世界標準時間 00:04
- 編輯時間：2017 年十二月三十日，世界標準時間 00:04
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaPackageV2FullAccess

描述：提供「 AWS 元素 MediaPackage V2」資源的完整存取權。

AWSElementalMediaPackageV2FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaPackageV2FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 7 月 25 日, 20:29
- 編輯時間：世界標準時間 2023 年 7 月 25 日晚上 20:29
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaPackageV2ReadOnly

描述：提供 AWS 元素 MediaPackage V2 資源的唯讀存取權。

AWSElementalMediaPackageV2ReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaPackageV2ReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 7 月 25 日, 20:31
- 編輯時間：世界標準時間 2023 年 7 月 25 日晚上 20:31
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaStoreFullAccess

說明：提供對所有 MediaStore API 的完整讀取和寫入存取

`AWSElementalMediaStoreFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElementalMediaStoreFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 5 日, 23:15 世界標準時間
- 編輯時間:2018 年 3 月 5 日, 世界標準時間 23:15
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaStoreReadOnly

說明：提供 MediaStore API 的唯讀權限

`AWSElementalMediaStoreReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`AWSElementalMediaStoreReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 8 日, 世界標準時間 19:48
- 編輯時間：2018 年 3 月 8 日，世界標準時間 19:48
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaTailorFullAccess

描述：提供 AWS 元素 MediaTailor 資源的完整存取權

AWSElementalMediaTailorFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaTailorFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月二十三日，世界標準時間 00:04
- 編輯時間：2021 年十一月二十三日，世界標準時間 00:04
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSElementalMediaTailorReadOnly

描述：提供 AWS 元素 MediaTailor 資源的唯讀存取權

AWSElementalMediaTailorReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSElementalMediaTailorReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月二十三日，世界標準時間 00:05
- 編輯時間：2021 年十一月二十三日，世界標準時間 00:05
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSEnhancedClassicNetworkingMangementPolicy

說明：啟用增強型傳統網路管理功能的原則。

AWSEnhancedClassicNetworkingMangementPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年 9 月 20 日，世界標準時間 17:29
- 編輯時間：2017 年 9 月 20 日，世界標準時間 17:29
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSEntityResolutionConsoleFullAccess

描述：提供主控台對「 AWS 實體解析」和相關服務的完整存取權。

AWSEntityResolutionConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSEntityResolutionConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 8 月 17 日, 17:54
- 編輯時間：世界標準時間 2023 年 10 月 16 日下午 18:46
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSEntityResolutionConsoleReadOnlyAccess

描述：透過提供「 AWS 實體解析」的唯讀存取權 AWS Management Console。

AWSEntityResolutionConsoleReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSEntityResolutionConsoleReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 8 月 17 日, 18:18
- 編輯時間：世界標準時間 2023 年 8 月 17 日下午 18 時 18 分
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFaultInjectionSimulatorEC2Access

說明：此政策授予 EC2 和其他執行 FIS 動作所需服務的故障注入模擬器服務權限。

AWSFaultInjectionSimulatorEC2Access是AWS 受管理的策略。

使用此政策

您可以附加AWSFaultInjectionSimulatorEC2Access至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2022 年 10 月 26 日，世界標準時間 20:39
- 編輯時間：世界標準時間 2023 年 11 月 27 日，下午 3:08
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFaultInjectionSimulatorECSAccess

描述：此原則授與 ECS 和其他執行 FIS 動作所需服務的「錯誤注入模擬器服務」權限。

AWSFaultInjectionSimulatorECSAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSFaultInjectionSimulatorECSAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2022 年 10 月 26 日，世界標準時間 20:37
- 編輯時間:世界標準時間 2024 年 1 月 25 日, 16:16
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFaultInjectionSimulatorEKSAccess

說明：此原則授與 EKS 中的錯誤注入模擬器服務權限，以執行 FIS 動作的其他必要服務。

AWSFaultInjectionSimulatorEKSAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSFaultInjectionSimulatorEKSAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2022 年 10 月 26 日，世界標準時間 20:34
- 編輯時間：世界標準時間 2023 年 11 月 13 日，16:44
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFaultInjectionSimulatorNetworkAccess

說明：此政策授予 EC2 聯網和其他必要服務中的故障注入模擬器服務權限，以執行 FIS 動作。

AWSFaultInjectionSimulatorNetworkAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSFaultInjectionSimulatorNetworkAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2022 年 10 月 26 日，世界標準時間 20:32
- 編輯時間:世界標準時間 2024 年 1 月 25 日, 16:07
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFaultInjectionSimulatorRDSAccess

描述：此原則會授與 RDS 中的錯誤插入模擬器服務權限，以執行 FIS 動作的其他必要服務。

AWSFaultInjectionSimulatorRDSAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSFaultInjectionSimulatorRDSAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：2022 年 10 月 26 日
- 編輯時間：世界標準時間：2023 年 11 月 13 日，下午 16:23
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFaultInjectionSimulatorSSMAccess

說明：此原則會授與 SSM 和其他必要服務中的錯誤插入模擬器服務權限，以執行 FIS 動作。

AWSFaultInjectionSimulatorSSMAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSFaultInjectionSimulatorSSMAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略

- **創建時間**：2022 年 10 月 26 日，世界標準時間下午 3:33
- **編輯時間**:2023 年 6 月 2 日, 世界標準時間 22:55
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFinSpaceServiceRolePolicy

說明：啟用 Amazon 存取 AWS 服務 和使用或管理資源的政策 FinSpace

AWSFinSpaceServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2023 年 5 月 12 日, 世界標準時間 16:42
- 編輯時間：世界標準時間 2023 年 12 月 1 日晚上 9 時 05 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFMAdminFullAccess

說明： AWS FM 管理員的完整存取權

AWSFMAdminFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSFMAdminFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 9 日, 世界標準時間 18:06
- 編輯時間：2022 年 10 月 20 日，世界標準時間 23:39
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFMAdminReadOnlyAccess

說明：允許監控 AWS FM 操作的 AWS FM 管理員的唯讀權限

AWSFMAdminReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSFMAdminReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**:2018 年 5 月 9 日, 世界標準時間 20:07
- **編輯時間**：2022 年 10 月 31 日，世界標準時間 22:42
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSFMMemberReadOnlyAccess

說明：針對 AWS Firewall Manager 員成員帳戶提供 AWS WAF 動作的唯讀存取權

AWSFMMemberReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSFMMemberReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 9 日, 世界標準時間 21:05
- 編輯時間:2018 年 5 月 9 日, 世界標準時間 21:05
- ARN: arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSForWordPressPluginPolicy

描述：對於 WordPress 插件 AWS 的管理策略

AWSForWordPressPluginPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSForWordPressPluginPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十月三十日, 00:27 世界標準時
- 編輯時間:2020 年 1 月 20 日, 世界標準時間 23:20
- ARN: arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGitSyncServiceRolePolicy

說明：允許 AWS 程式碼連線同步 Git 儲存庫內容的政策

AWSGitSyncServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 16 日下午 17 點 5 分
- 編輯時間:2024 年 4 月 26 日, 世界標準時間 18:12
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGlobalAcceleratorSLRPolicy

說明：將權限授與 AWS 全域加速器以管理 EC2 彈性網路界面和安全群組的政策。

AWSGlobalAcceleratorSLRPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 4 月 5 日, 世界標準時間 19:39
- 編輯時間：世界標準時間 2023 年 9 月 12 日，16:45
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGlueConsoleFullAccess

說明：提供透過 AWS Glue 的完整存取權 AWS Management Console

`AWSGlueConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSGlueConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 8 月 14 日, 世界標準時間 13:37
- 編輯時間：世界標準時間 7 月 14 日（世界標準時間）14:37
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGlueConsoleSageMakerNotebookFullAccess

描述：透過 Sageemaker 筆記本執行個體的 AWS Management Console 和存取權，提供 AWS Glue 的完整存取權。

AWSGlueConsoleSageMakerNotebookFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSGlueConsoleSageMakerNotebookFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 5 日, 世界標準時間 17:52
- 編輯時間：2021 年 7 月 15 日，世界標準時間 15:24
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AwsGlueDataBrewFullAccessPolicy

描述：提供 DataBrew 透過 AWS Glue 的完整存取權 AWS Management Console。還提供對相關服務（例如 S3，KMS，Glue）的選擇訪問權限。

AwsGlueDataBrewFullAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AwsGlueDataBrewFullAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二零年十一月十一日, 16:51 世界標準
- 編輯時間：2022 年 2 月 4 日，世界標準時間下午 18:28
- ARN: arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGlueDataBrewServiceRole

描述：此政策授予粘合在用戶的膠水數據目錄上執行操作的權限，此政策還提供了 ec2 操作的許可，以允許膠水創建 ENI 以連接到 VPC 中的資源，還允許膠水訪問湖形中的註冊數據以及訪問用戶的 cloudwatch 的權限

AWSGlueDataBrewServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AWSGlueDataBrewServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略

- **創建時間**：二零二零年十二月四日 21:26 世界標準時間
- **編輯時間**：世界標準時間 2024 年 3 月 20 日 23:28
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGlueSchemaRegistryFullAccess

說明：提供 AWS Glue 綱要登錄服務的完整存取權

AWSGlueSchemaRegistryFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSGlueSchemaRegistryFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年十一月二十日，世界標準時間 00:19
- 編輯時間：2020 年十一月二十日，世界標準時間 00:19
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGlueSchemaRegistryReadonlyAccess

說明：提供 AWS Glue 綱要登錄服務的唯讀存取權

AWSGlueSchemaRegistryReadonlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSGlueSchemaRegistryReadonlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年十一月二十日，世界標準時間 00:20
- 編輯時間：2020 年十一月二十日，世界標準時間 00:20
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGlueServiceNotebookRole

描述：允許客戶管理筆記型電腦伺服器之 AWS Glue 服務角色的政策

AWSGlueServiceNotebookRole是AWS 受管理的策略。

使用此政策

您可以附加AWSGlueServiceNotebookRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 8 月 14 日, 世界標準時間 13:37
- 編輯時間：世界標準時間 2023 年 10 月 9 日，下午 15:59
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGlueServiceRole

說明：允許存取 EC2、S3 和雲端手錶日誌等相關服務的 AWS Glue 服務角色政策

AWSGlueServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AWSGlueServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 8 月 14 日, 世界標準時間 13:37
- 編輯時間：世界標準時間 2023 年 9 月 11 日，16:39
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AwsGlueSessionUserRestrictedNotebookPolicy

描述：提供權限，讓使用者只能建立和使用與使用者相關聯的記事本工作階段。此原則也包含明確允許使用者傳遞受限制 Glue 工作階段角色的權限。

AwsGlueSessionUserRestrictedNotebookPolicy是AWS 受管理的策略。

使用此政策

您可以附加AwsGlueSessionUserRestrictedNotebookPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 4 月 18 日, 下午 3:24
- 編輯時間:2023 年 11 月 22 日, 01:32 世界標準時間
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AwsGlueSessionUserRestrictedNotebookServiceRole

描述：提供對工作階段以外的所有 AWS Glue 資源的完整存取權。允許使用者僅建立並使用與使用者相關聯的筆記本工作階段。此原則也包含 AWS Glue 在其他 AWS 服務中管理 Glue 資源所需的其他權限。

`AwsGlueSessionUserRestrictedNotebookServiceRole`是AWS 受管理的策略。

使用此政策

您可以附加`AwsGlueSessionUserRestrictedNotebookServiceRole`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2022 年 4 月 18 日，世界標準時間下午 3:27
- 編輯時間：2022 年 4 月 18 日，世界標準時間下午 3:27
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AwsGlueSessionUserRestrictedPolicy

描述：提供權限，讓使用者只能建立和使用與使用者相關聯的互動式工作階段。此原則也包含明確允許使用者傳遞受限制 Glue 工作階段角色的權限。

AwsGlueSessionUserRestrictedPolicy是AWS 受管理的策略。

使用此政策

您可以附加AwsGlueSessionUserRestrictedPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 4 月 14 日，世界標準時間 21:31
- 編輯時間:世界標準時間 2024 年 4 月 29 日, 22:45
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AwsGlueSessionUserRestrictedServiceRole

描述：提供對工作階段以外的所有 AWS Glue 資源的完整存取權。允許使用者建立並僅使用與使用者相關聯的互動式工作階段。此原則也包含 Glue 在其他 AWS 服務中管理 AWS Glue 資源所需的其他權限

`AwsGlueSessionUserRestrictedServiceRole`是AWS 受管理的策略。

使用此政策

您可以附加`AwsGlueSessionUserRestrictedServiceRole`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2022 年 4 月 14 日, 21:30
- 編輯時間：世界標準時間 2024 年 4 月 29 日 22:51
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStatementActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${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/*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGrafanaAccountAdministrator

描述：提供 Amazon Grafana 內部的存取權，以建立和管理整個組織的工作區。

AWSGrafanaAccountAdministrator是AWS 受管理的策略。

使用此政策

您可以附加AWSGrafanaAccountAdministrator至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 2 月 23 日，世界標準時間 00:20
- 編輯時間：世界標準時間 2022 年 2 月 15 日上午 22 時 36 分
- ARN: arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGrafanaConsoleReadOnlyAccess

描述：訪問 Amazon Grafana 的只讀操作。

AWSGrafanaConsoleReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSGrafanaConsoleReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 2 月 23 日，世界標準時間 00:10
- 編輯時間：世界標準時間 2022 年 2 月 15 日晚上 22 點 30 分
- ARN: arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGrafanaWorkspacePermissionManagement

描述：僅提供更新 AWS Grafana 工作區之使用者和群組權限的功能。

AWSGrafanaWorkspacePermissionManagement是AWS 受管理的策略。

使用此政策

您可以附加AWSGrafanaWorkspacePermissionManagement至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 2 月 23 日，世界標準時間 00:15
- 編輯時間:世界標準時間 2023 年 3 月 15 日, 22:17
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGrafanaWorkspacePermissionManagementV2

說明：提供更新 Amazon 受管 Grafana 工作區的 IAM 身分中心 (IdC) 使用者和群組許可的功能。

AWSGrafanaWorkspacePermissionManagementV2是AWS 受管理的策略。

使用此政策

您可以附加AWSGrafanaWorkspacePermissionManagementV2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2024 年 1 月 5 日, 18:39
- 編輯時間:2024 年 1 月 5 日, 世界標準時間 18:39
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGreengrassFullAccess

說明：此原則提供 AWS Greengrass 組態、管理和部署動作的完整存取權

AWSGreengrassFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSGreengrassFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 5 月 3 日，世界標準時間 00:47

- 編輯時間：2017 年 5 月 3 日，世界標準時間 00:47
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGreengrassReadOnlyAccess

說明：此原則提供 AWS Greengrass 組態、管理和部署動作的唯讀存取權

`AWSGreengrassReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加AWSGreengrassReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 30 日, 世界標準時間 16:01
- 編輯時間：2018 年 10 月 30 日，世界標準時間 16:01
- ARN: arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGreengrassResourceAccessRolePolicy

描述： AWS Greengrass 服務角色的政策，允許存取相關服務，包括 AWS Lambda 和 AWS IoT 物件陰影。

AWSGreengrassResourceAccessRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSGreengrassResourceAccessRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 2 月 14 日, 世界標準時間 21:17
- 編輯時間：2018 年十一月十四日，世界標準時間 00:35
- ARN: arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSGroundStationAgentInstancePolicy

說明：提供 Dataflow 端點執行個體使用權限，以使用 G AWS round Station 台代理程式

AWSGroundStationAgentInstancePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSGroundStationAgentInstancePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 3 月 29 日下午 3:23
- 編輯時間：世界標準時間 2023 年 3 月 29 日下午 3:23
- ARN: arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSHealth_EventProcessorServiceRolePolicy

描述：允許「 AWS Health」啟用「Health」事件處理器功能。

`AWSHealth_EventProcessorServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 1 月 13 日，19:24
- 編輯時間：世界標準時間 2023 年 1 月 13 日，19:24
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSHealthFullAccess

描述：允許完整存取 AWS Health Api 和通知以及 Personal Health Dashboard

AWSHealthFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSHealthFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一六年十二月六日，世界標準時間中
- 編輯時間:2020 年十一月十六日, 世界標準時間 18:11
- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSHealthImagingFullAccess

描述：提供對 AWS Health 成像服務的完整存取權。

AWSHealthImagingFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSHealthImagingFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 7 月 25 日, 23:39
- 編輯時間：世界標準時間 2023 年 7 月 25 日 23:39
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSHealthImagingReadOnlyAccess

描述：提供 AWS Health 成像服務的唯讀存取權。

AWSHealthImagingReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSHealthImagingReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 7 月 25 日 23:40
- 編輯時間：世界標準時間 2023 年 8 月 1 日下午 3:18
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIAMIdentityCenterAllowListForIdentityContext

描述：提供 IAM 身分中心身分內容所允許的角色所允許的動作清單。 AWS 安全性權杖服務 (AWS STS) 會自動將此原則附加至假設的角色。身份上下文作為傳遞 ProvidedContext。

`AWSIAMIdentityCenterAllowListForIdentityContext`是AWS 受管理的策略。

使用此政策

您可以附加`AWSIAMIdentityCenterAllowListForIdentityContext`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 11 月 8 日，下午 3:21
- 編輯時間：世界標準時間 2024 年 4 月 30 日 09:31
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
```

```
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIdentitySyncFullAccess

說明：授與身分同步服務的完整存取權

AWSIdentitySyncFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIdentitySyncFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2022 年 3 月 23 日 23:29
- 編輯時間：2022 年 3 月 23 日，世界標準時間 23:29
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIdentitySyncReadOnlyAccess

說明：身分同步服務的唯讀存取權

AWSIdentitySyncReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIdentitySyncReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2022 年 3 月 23 日 23:29
- 編輯時間：2022 年 3 月 23 日，世界標準時間 23:29
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSImageBuilderFullAccess

描述：提供對所有 AWS Image Builder 動作的完整存取權，以及對相關 AWS 服務的資源範圍存取權。

AWSImageBuilderFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSImageBuilderFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月二十日, 18:25 世界標準
- 編輯時間：2021 年 4 月 13 日，世界標準時間 17：33
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSImageBuilderReadOnlyAccess

描述：提供對所有「 AWS Image Builder」動作的唯讀存取權。

`AWSImageBuilderReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSImageBuilderReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月十九日, 世界標準時間
- 編輯時間：2019 年十二月十九日，世界標準時間 22:29

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

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSImportExportFullAccess

描述：提供在下建立之工作的讀取和寫入存取權 AWS 帳戶。

AWSImportExportFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSImportExportFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AWSImportExportFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSImportExportReadOnlyAccess

描述：提供在下建立之工作的唯讀存取權 AWS 帳戶。

AWSImportExportReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSImportExportReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIncidentManagerIncidentAccessServiceRolePolicy

說明：授與事件管理員權限，以便在管理事件時呼叫其他 AWS 服務。

AWSIncidentManagerIncidentAccessServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSIncidentManagerIncidentAccessServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2023 年 11 月 13 日，世界標準時間 00:01
- 編輯時間：世界標準時間 2024 年 2 月 20 日 23:02
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIncidentManagerResolverAccess

描述：此原則授與權限來啟動、檢視和更新事件，並具有對自訂時間表事件和相關項目的完整存取權。將此原則指派給將建立並解決事件的使用者。

AWSIncidentManagerResolverAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIncidentManagerResolverAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 5 月 10 日, 06:12 世界標準時間
- 編輯時間:2021 年 5 月 10 日, 06:12 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIncidentManagerServiceRolePolicy

說明：此原則授與事件管理員權限，以代表您管理事件記錄和相關資源。

AWSIncidentManagerServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 5 月 10 日, 3:34 世界標準時間
- 編輯時間：世界標準時間（世界標準時間）12 月 5 日
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoT1ClickFullAccess

描述：提供 AWS IoT 1-Click 式的完整存取權。

AWSIoT1ClickFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoT1ClickFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 11 日, 世界標準時間 22:10
- 編輯時間:2018 年 5 月 11 日, 世界標準時間 22:10

- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoT1ClickReadOnlyAccess

描述：提供 AWS IoT 1-Click 的唯讀存取權。

`AWSIoT1ClickReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加AWSIoT1ClickReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 11 日, 21:49 世界標準時間
- 編輯時間:2018 年 5 月 11 日, 世界標準時間 21:49
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTAnalyticsFullAccess

描述：提供 IoT Analytics 的完整存取權。

AWSIoTAnalyticsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTAnalyticsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 18 日, 世界標準時間 23:02
- 編輯時間:2018 年 6 月 18 日, 世界標準時間 23:02
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTAnalyticsReadOnlyAccess

描述：提供 IoT Analytics 的唯讀存取權。

AWSIoTAnalyticsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTAnalyticsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 18 日, 21:37 世界標準時間
- 編輯時間:2018 年 6 月 18 日, 世界標準時間 21:37
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTConfigAccess

描述：此原則可提供 AWS IoT 設定動作的完整存取權

AWSIoTConfigAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTConfigAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:十月二十七日, 21:52 世界標準時間
- 編輯時間：2019 年 9 月 27 日，世界標準時間 20:48
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigAccess

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTConfigReadOnlyAccess

說明：此原則提供 AWS IoT 設定動作的唯讀存取權

AWSIoTConfigReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTConfigReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:十月二十七日, 21:52 世界標準時間
- 編輯時間：2019 年 9 月 27 日，世界標準時間 20:52
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDataAccess

描述：此原則可提供 AWS IoT 訊息動作的完整存取權

AWSIoTDataAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTDataAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:十月二十七日, 21:51 世界標準時間
- 編輯時間：2021 年 6 月 23 日，世界標準時間 21:34
- ARN: arn:aws:iam::aws:policy/AWSIoTDataAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

描述：提供 IoT 物件群組的寫入存取權，以及 IoT 憑證的讀取存取權，以便執行新增的 THINGS_TO_GROUP 緩和動作

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2019 年 8 月 7 日, 世界標準時間 17:55
- 編輯時間:2019 年 8 月 7 日, 世界標準時間 17:55
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceDefenderAudit

說明：提供 IoT 和相關資源的讀取權限

AWSIoTDeviceDefenderAudit是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTDeviceDefenderAudit至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 7 月 18 日, 世界標準時間 21:17
- 編輯時間：2019 年 11 月 25 日，世界標準時間 23:52
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

說明：提供存取權以啟用 IoT 記錄以執行 EABLE_IOT_LOG 緩解動作

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2019 年 8 月 7 日, 世界標準時間 17:04
- 編輯時間:2019 年 8 月 7 日, 世界標準時間 17:04
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

描述：提供 SNS 主題的訊息發佈存取權，以執行發佈 _FINDING_TO_SNS 緩和動作

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2019 年 8 月 7 日, 世界標準時間 17:04
- 編輯時間:2019 年 8 月 7 日, 世界標準時間 17:04
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

描述：提供 IoT 原則的寫入存取權，以便執行替換 _ 預設 _ 政策 _ 版本緩解動作

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`是AWS 受管理的策略。

使用此政策

您可以附加`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2019 年 8 月 7 日, 世界標準時間 17:04
- 編輯時間:2019 年 8 月 7 日, 世界標準時間 17:04
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceDefenderUpdateCACertMitigationAction

描述：提供 IoT CA 憑證的寫入存取權，以便執行更新 _ CA_ 憑證緩解動作

AWSIoTDeviceDefenderUpdateCACertMitigationAction是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTDeviceDefenderUpdateCACertMitigationAction至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2019 年 8 月 7 日, 世界標準時間 17:05

- 編輯時間:2019 年 8 月 7 日, 世界標準時間 17:05
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

描述：提供 IoT 憑證的寫入存取權，以便執行更新 _ 證書緩解動作

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2019 年 8 月 7 日, 世界標準時間 17:06
- 編輯時間:2019 年 8 月 7 日, 世界標準時間 17:06
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceTesterForFreeRTOSFullAccess

說明：允許 AWS IoT 裝置測試人員透過允許存取 IoT、S3 和 IAM 等服務來執行 FreeRTOS 資格套件

`AWSIoTDeviceTesterForFreeRTOSFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSIoTDeviceTesterForFreeRTOSFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 2 月 12 日, 世界標準時間 20:33
- 編輯時間：世界標準時間 2023 年 8 月 10 日 20:30
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTDeviceTesterForGreengrassFullAccess

說明：允許 AWS IoT 裝置測試人員透過允許存取相關服務 (包括 Lambda、IoT、API Gateway、IAM) 來執行 AWS Greengrass 認證套件

AWSIoTDeviceTesterForGreengrassFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTDeviceTesterForGreengrassFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 2 月 20 日, 世界標準時間 21:21
- 編輯時間：2020 年 6 月 25 日, 世界標準時間 17:01
- ARN: arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTEventsFullAccess

描述：提供 IoT Events 的完整存取權。

AWSIoTEventsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTEventsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一九年一月十日, 世界標準時間 22:51
- 編輯時間：2019 年 1 月 10 日，世界標準時間 22:51
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTEventsReadOnlyAccess

描述：提供 IoT Events 的唯讀存取權。

AWSIoTEventsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTEventsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年一月十日, 世界標準時間 22:50
- 編輯時間：2019 年 9 月 23 日，世界標準時間 17:22
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:Describe*",
        "iotevents:List*"
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTFleetHubFederationAccess

說明：IoT 叢集中樞應用程式的同盟存取

AWSIoTFleetHubFederationAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTFleetHubFederationAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年十二月十五日, 世界標準時間 8:08
- 編輯時間：2022 年 4 月 4 日，世界標準時間 18:03
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTFleetwiseServiceRolePolicy

描述：授與輔助功能使用或管理的 AWS 資源和中繼資 AWSIoTFleetwise 料的權限

AWSIoTFleetwiseServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2022 年 9 月 21 日，世界標準時間 23:27
- 編輯時間：2022 年 9 月 21 日，世界標準時間 23:27
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTFullAccess

描述：此原則可提供 AWS IoT 組態和訊息動作的完整存取權

AWSIoTFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 10 月 8 日, 下午 3:19
- 編輯時間：2022 年 5 月 19 日，世界標準時間 21:39
- ARN: arn:aws:iam::aws:policy/AWSIoTFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "iot:*",
        "iotjobsdata:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTLogging

描述：允許建立 Amazon 日 CloudWatch 誌群組和將日誌串流到群組

AWSIoTLogging是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTLogging至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:十月 8 日, 下午 3:17 世界標準時間
- 編輯時間:2015 年 10 月 8 日, 15:17 世界標準時間
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTLogging

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTOTAUpdate

描述：允許存取建立 AWS IoT Job 並描述 AWS 程式碼簽署者工作

AWSIoTOTAUpdate是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTOTAUpdate至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年十二月二十日, 世界標準時間 20:36
- 編輯時間：2017 年十二月二十日，世界標準時間 20:36
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIotRoboRunnerFullAccess

描述：此原則授與允許完整存取 Its 的 AWS 權限 RoboRunner。

AWSIotRoboRunnerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIotRoboRunnerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年十一月二十九日，3:54 世界標準時間
- 編輯時間：世界標準時間 2023 年 2 月 23 日下午 18:34
- ARN: arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIotRoboRunnerReadOnly

描述：此原則授與允許 I AWS ot 唯讀存取權的權限 RoboRunner。

AWSIotRoboRunnerReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSIotRoboRunnerReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年十一月二十九日, 3:43 世界標準時間
- 編輯時間：2022 年十一月十六日，世界標準時間 20:51
- ARN: arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIotRoboRunnerServiceRolePolicy

描述：允許 AWS IoT RoboRunner 代表客戶管理關聯的 AWS 資源。

AWSIotRoboRunnerServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 2 月 21 日，16:56
- 編輯時間：世界標準時間 2023 年 2 月 21 日，16:56
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTRuleActions

描述：允許存取 AWS IoT 規則動作中支援的所有 AWS 服務

AWSIoTRuleActions是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTRuleActions至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 10 月 8 日, 15:14 世界標準時間
- 編輯時間:2018 年 1 月 16 日, 世界標準時間 19:28
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTSiteWiseConsoleFullAccess

描述：提供 SiteWise 使用管理 AWS IoT 的完整存取權 AWS Management Console。請注意，此原則也授予存取權以建立和列出與 AWS IoT 搭配使用的資料存放區 SiteWise (例如 AWS IoT Analytics)、清單和檢視 AWS IoT Greengrass 資源、列出和修改 AWS Secrets Manager 秘密、擷取 AWS IoT 物件陰影、列出具有特定標籤的資源，以及建立和使用 IoT 的服務連結角色。 AWS SiteWise

`AWSIoTSiteWiseConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSIoTSiteWiseConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 5 月 31 日, 世界標準時間 21:37
- 編輯時間：2019 年 5 月 31 日，世界標準時間 21:37
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTSiteWiseFullAccess

描述：提供 IoT 的完整存取權 SiteWise。

AWSIoTSiteWiseFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTSiteWiseFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 12 月 4 日, 世界標準時間 20:53
- 編輯時間：2018 年 12 月 4 日，世界標準時間 20:53
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTSiteWiseMonitorPortalAccess

描述：此原則授與存取 AWS IoT SiteWise 資產和資產資料、建立 AWS IoT SiteWise 監視器資源以及列出 AWS SSO 使用者的權限。

`AWSIoTSiteWiseMonitorPortalAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSIoTSiteWiseMonitorPortalAccess`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 5 月 19 日, 世界標準時間 20:01
- 編輯時間：2020 年 5 月 19 日，世界標準時間 20:01
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTSiteWiseMonitorServiceRolePolicy

描述：此角色授予 AWS IoT SiteWise 監視器權限，以存取您的 AWS IoT 資 SiteWise 產和資產屬性，以及透過 AWS AWS IoT SiteWise 入口網站建立 IoT Sitewise 專案、儀表板和存取政策。

`AWSIoTSiteWiseMonitorServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：二零一九年十一月十四日，世界時間 00:59
- 編輯時間：2019 年十二月十三日，世界標準時間 22:19
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTSiteWiseReadOnlyAccess

描述：提供 IoT 的唯讀存取權 SiteWise。

AWSIoTSiteWiseReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTSiteWiseReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 12 月 4 日, 世界標準時間 20:55
- 編輯時間：2022 年 9 月 16 日，世界標準時間 19:05
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotsitewise:Get*",
        "iotsitewise:BatchGet*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTThingsRegistration

說明：此原則允許使用者使用 AWS IoT StartThingRegistrationTask API 大量註冊事物

`AWSIoTThingsRegistration`是AWS 受管理的策略。

使用此政策

您可以附加`AWSIoTThingsRegistration`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 12 月 1 日, 世界標準時間 20:21
- 編輯時間：2020 年 10 月 5 日，世界標準時間 19:20
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTTwinMakerServiceRolePolicy

描述：允許 AWS IoT TwinMaker 呼叫其他 AWS 服務，並代表您同步其資源。

`AWSIoTTwinMakerServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 13 日，18:59
- 編輯時間:2023 年 11 月 13 日, 世界標準時間 18:59
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TwinMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",
```

```
        "iottwinmaker:DeleteEntity",
        "iottwinmaker:ListEntities",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:CreateComponentType",
        "iottwinmaker:UpdateComponentType",
        "iottwinmaker:DeleteComponentType",
        "iottwinmaker:ListComponentTypes"
      ],
      "Resource" : [
        "arn:aws:iottwinmaker:*:*:workspace/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTWirelessDataAccess

描述：允許存取 AWS IoT Wireless 裝置的相關身分資料。

`AWSIoTWirelessDataAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSIoTWirelessDataAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- 創建時間:2020 年十二月十五日, 世界標準時間 15:31
- 編輯時間：2020 年十二月十五日，世界標準時間 15:31
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTWirelessFullAccess

描述：允許相關聯的身分完整存取所有 AWS IoT Wireless 作業。

`AWSIoTWirelessFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTWirelessFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十五日, 世界標準時間 15:27
- 編輯時間:2020 年十二月十五日, 世界標準時間 15:27
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTWirelessFullPublishAccess

描述：提供 IoT Wireless 完整存取權，以代表您發佈至 IoT 規則引擎。

AWSIoTWirelessFullPublishAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTWirelessFullPublishAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十五日, 世界標準時間 15:29
- 編輯時間：2020 年十二月十五日，世界標準時間 15:29
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTWirelessGatewayCertManager

描述：允許建立、列出和描述 IoT 憑證的相關身分存取權

AWSIoTWirelessGatewayCertManager是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTWirelessGatewayCertManager至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年十二月十五日, 世界標準時間 15:30
- 編輯時間：2020 年十二月十五日，世界標準時間 15:30
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTWirelessLogging

描述：允許相關聯的身分建立 Amazon CloudWatch 日誌群組，並將日誌串流到群組。

AWSIoTWirelessLogging是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTWirelessLogging至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十五日, 世界標準時間 15:32
- 編輯時間：2020 年十二月十五日，世界標準時間 15:32
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessLogging

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIoTWirelessReadOnlyAccess

描述：允許 AWS IoT 無線的相關身份唯讀存取。

AWSIoTWirelessReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIoTWirelessReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十五日, 世界標準時間 15:28
- 編輯時間：2020 年十二月十五日，世界標準時間 15:28
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIPAMServiceRolePolicy

描述：允許 VPC IP 位址管理員存取 VPC 資源，並代表您與 Organ AWS izations 整合。

AWSIPAMServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年十一月三十日, 世界標準時間 19:08
- 編輯時間：世界標準時間 2023 年 11 月 8 日，19:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIQContractServiceRolePolicy

說明： AWS IQ 用於代表客戶執行付款請求

AWSIQContractServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 8 月 22 日, 世界標準時間 19:28
- 編輯時間：2019 年 8 月 22 日，世界標準時間 19:28
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIQFullAccess

說明：提供對 AWS IQ 的完整存取

AWSIQFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSIQFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 4 月 4 日, 23:13 世界標準時間
- 編輯時間：2019 年 9 月 25 日，世界標準時間 20:22
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSIQPermissionServiceRolePolicy

描述：允許 AWS IQ 管理 I AWS Q 專家承擔的角色。

AWSIQPermissionServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 8 月 22 日, 世界標準時間 19:36
- 編輯時間：2019 年 8 月 22 日，世界標準時間 19:36
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

描述：允許存取 AWS KMS 自訂金鑰存放區所需的 AWS 服務和資源

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月十四日, 世界標準時間 20:10
- 編輯時間：世界標準時間 2023 年 11 月 10 日，下午 19:03
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

描述：可讓 AWS KMS 同步處理多區域金鑰的共用內容。

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 6 月 16 日, 世界標準時間 15:37
- 編輯時間：2021 年 6 月 16 日，世界標準時間 15:37
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSKeyManagementServicePowerUser

說明：提供金 AWS 鑰管理服務 (KMS) 的存取權。

AWSKeyManagementServicePowerUser是AWS 受管理的策略。

使用此政策

您可以附加AWSKeyManagementServicePowerUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**:2015 年 2 月 6 日, 18:40 世界標準時間
- **編輯時間**：2017 年 3 月 7 日，世界標準時間 00:55
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLakeFormationCrossAccountManager

描述：透過 Lake Formation 提供跨帳戶存取 Glue 資源。還授予對其他必要服務的讀取權限，例如組織和資源存取管理員

AWSLakeFormationCrossAccountManager是AWS 受管理的策略。

使用此政策

您可以附加AWSLakeFormationCrossAccountManager至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 4 日, 世界標準時間 20:59
- 編輯時間：世界標準時間 2024 年 3 月 22 日 18:51
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLakeFormationDataAdmin

描述：授予 AWS Lake Formation 的管理權限和相關服務，例如 AWS Glue，以管理資料湖

AWSLakeFormationDataAdmin是AWS 受管理的策略。

使用此政策

您可以附加AWSLakeFormationDataAdmin至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 8 月 8 日, 17:33 世界標準時間
- 編輯時間：世界標準時間 2024 年 3 月 22 日下午 18:27
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambda_FullAccess

說明：授予 AWS Lambda 服務、 AWS Lambda 主控台功能和其他相關 AWS 服務的完整存取權。

AWSLambda_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSLambda_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十一月十七日, 世界標準時間 21:14
- 編輯時間：2020 年十一月十七日，世界標準時間 21:14
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
```

```
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambda_ReadOnlyAccess

說明：授予 AWS Lambda 服務、 AWS Lambda 主控台功能和其他相關 AWS 服務的唯讀存取權。

AWSLambda_ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSLambda_ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十一月十七日, 世界標準時間 21:10
- 編輯時間:世界標準時間 7 月 27 日, 下午 17 時 32 分
- ARN: arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaBasicExecutionRole

描述：提供 CloudWatch 記錄檔的寫入權限。

AWSLambdaBasicExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaBasicExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 4 月 9 日, 下午 3:03 世界標準時間
- 編輯時間:2015 年 4 月 9 日, 15:03 世界標準時間
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaDynamoDBExecutionRole

描述：提供 DynamoDB 串流的清單和讀取存取權限，以及記錄檔的寫入 CloudWatch 權限。

AWSLambdaDynamoDBExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaDynamoDBExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 4 月 9 日, 下午 3:09 世界標準時間
- 編輯時間:2015 年 4 月 9 日, 15:09 世界標準時間
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaENIManagementAccess

說明：提供 Lambda 函數的最低權限，以管理啟用 VPC 的 Lambda 函數所使用的 ENI (建立、描述、刪除)。

AWSLambdaENIManagementAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaENIManagementAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一六年十二月六日, 00:37 世界標準時
- 編輯時間:2020 年 10 月 1 日, 世界標準時間 20:07
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaExecute

說明：提供 PUT、取得 S3 的存取權限，以及對 CloudWatch 日誌的完整存取權限。

AWSLambdaExecute是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaExecute至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AWSLambdaExecute

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaFullAccess

說明：此原則位於淘汰路徑上。請參閱文檔以獲取指導：access-control-identity-basedhttps://docs.aws.amazon.com/lambda/latest/dg/ 提供對 Lambda、S3、DynamoDB 支援、 CloudWatch 指標和日誌的完整存取權。

AWSLambdaFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2017 年十一月二十七日，世界標準時間 23:22
- ARN: arn:aws:iam::aws:policy/AWSLambdaFullAccess

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaInvocation-DynamoDB

說明：提供 DynamoDB Streams 的讀取存取權限。

AWSLambdaInvocation-DynamoDB是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaInvocation-DynamoDB至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaKinesisExecutionRole

說明：提供 Kinesis 串流的清單和讀取存取權限，以及 CloudWatch 記錄的寫入權限。

AWSLambdaKinesisExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaKinesisExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 4 月 9 日, 下午 3:14 世界標準時間
- 編輯時間:2018 年十一月十九日, 世界標準時間 20:09
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaMSKExecutionRole

描述：提供在 VPC 中存取 MSK 叢集、管理 VPC 中的 ENI (建立、描述、刪除) 以及寫入記錄檔的權限所需的權限。 CloudWatch

AWSLambdaMSKExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaMSKExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 8 月 11 日, 世界標準時間 17:35
- 編輯時間：2022 年 8 月 2 日，世界標準時間 20:08
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaReplicator

說明：授予 Lambda 複寫器必要的權限，以便跨區域複寫函數

AWSLambdaReplicator是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 5 月 23 日, 世界標準時間 17:53
- 編輯時間：2017 年十二月八日，00:17 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaRole

說明： AWS Lambda 服務角色的預設政策。

AWSLambdaRole是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaSQSQueueExecutionRole

說明：提供 SQS 佇列的接收訊息、刪除訊息和讀取屬性存取權限，以及 CloudWatch 記錄檔的寫入權限。

AWSLambdaSQSQueueExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaSQSQueueExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 6 月 14 日, 世界標準時間 21:50
- 編輯時間:2018 年 6 月 14 日, 世界標準時間 21:50
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLambdaVPCAccessExecutionRole

描述：提供 Lambda 函數在存取 VPC 內的資源時執行的最低權限-建立、描述、刪除網路介面，以及將權限寫入 CloudWatch 記錄。

AWSLambdaVPCAccessExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AWSLambdaVPCAccessExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：二零一六年二月十一日 23:15 世界標準時間

- **編輯時間**：世界標準時間 2024 年 1 月 5 日 22:38
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLicenseManagerConsumptionPolicy

描述：提供權限，以允許存取使用者擁有權利的授權所需的 Lic AWS ense Manager API 動作。

AWSLicenseManagerConsumptionPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSLicenseManagerConsumptionPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年 8 月 11 日, 世界標準時間 23:18
- 編輯時間:2021 年 8 月 11 日, 世界標準時間 23:18
- ARN: arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

描述：允 AWS 許 License Manager Linux 訂閱服務代表您管理資源。

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間（世界標準時間）12 月 20 日
- 編輯時間：2022 年十二月二十日（世界標準時間）18:54
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLicenseManagerMasterAccountRolePolicy

描述：L AWS icense Manager 服務主要帳戶角色策略

AWSLicenseManagerMasterAccountRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月二十六日, 世界標準時間 19:03
- 編輯時間：2022 年 5 月 31 日，世界標準時間 20:50
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLicenseManagerMemberAccountRolePolicy

描述：L AWS icense Manager 服務成員帳戶角色策略

AWSLicenseManagerMemberAccountRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月二十六日, 世界標準時間 19:04
- 編輯時間：2019 年十一月十五日，世界標準時間 22:09
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLicenseManagerServiceRolePolicy

描述：L AWS icense Manager 服務預設角色原則

`AWSLicenseManagerServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月二十六日, 世界標準時間 19:02
- 編輯時間:2021 年 7 月 30 日, 世界標準時間 1:43
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

描述：允 AWS 許 License Manager 使用者訂閱服務代表您管理資源。

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 7 月 30 日, 星期五
- 編輯時間：2022 年十一月二十一日，世界標準時間 19:51
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:productCode" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
            "77yzkpa7kvee1y1tt7wnsdwoc"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SSMDocumentExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunPowerShellScript"
      ]
    },
    {
      "Sid" : "SSMInstanceExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSM2ServicePolicy

描述：允許 AWS M2 代表您管理 AWS 資源。

AWSM2ServicePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2022 年 6 月 7 日，世界標準時間 20:26
- 編輯時間：2022 年 6 月 7 日，世界標準時間 20:26
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSManagedServices_ContactsServiceRolePolicy

描述：允許 AWS 受管理的服務讀取 AWS 資源上的標籤值

AWSManagedServices_ContactsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2023 年 3 月 23 日, 17:07
- 編輯時間：世界標準時間 2023 年 3 月 23 日下午 17 時 7 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

描述： AWS Managed Services-管理偵探控制項基礎結構的政策

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2022 年十二月十九日 23:11

- 編輯時間：2022 年十二月十九日，世界標準時間 23:11
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSManagedServices_EventsServiceRolePolicy

描述：啟用 AMS 事件處理器功能的 AWS 受管理服務政策。

AWSManagedServices_EventsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2023 年 2 月 7 日, 18:41
- 編輯時間：世界標準時間 2023 年 2 月 7 日下午 18:41
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSManagedServicesDeploymentToolkitPolicy

描述：允許 AWS Managed Services 代表您管理部署工具組。

`AWSManagedServicesDeploymentToolkitPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2022 年 6 月 9 日，世界標準時間 18:33
- 編輯時間:2024 年 4 月 4 日, 世界標準時間 20:41
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceAmiIngestion

描述： AWS Marketplace 允許複製您的 Amazon 機器映像（AMI），以便列出它們 AWS Marketplace

AWSMarketplaceAmiIngestion是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceAmiIngestion至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 9 月 25 日，世界標準時間 20:55
- 編輯時間：2020 年 9 月 25 日，世界標準時間 20:55
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceDeploymentServiceRolePolicy

描述：允許 AWS Marketplace 為您訂閱的產品創建和管理賣方部署參數 AWS Marketplace。

AWSMarketplaceDeploymentServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 15 日 23:34
- 編輯時間：世界標準時間 2023 年 11 月 15 日 23:34
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceFullAccess

說明：提供訂閱和取消訂閱 AWS Marketplace 軟體的功能、允許使用者從 Marketplace「您的軟體」頁面管理 Marketplace 軟體執行個體，以及提供 EC2 的管理存取權。

AWSMarketplaceFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2015 年 2 月 11 日, 17:21
- 編輯時間：世界標準時間 2022 年 3 月 4 日下午 17 時 4 分
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceGetEntitlements

描述：提供權利的讀取存取 AWS Marketplace 權

AWSMarketplaceGetEntitlements是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceGetEntitlements至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 3 月 27 日, 世界標準時間 19:37
- 編輯時間:2024 年 4 月 5 日, 01:27 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceImageBuildFullAccess

描述：提供 AWS Marketplace 私人映像建置功能的完整存取權。除了創建私有映像之外，它還提供向映像添加標籤，啟動和終止 ec2 實例的許可。

AWSMarketplaceImageBuildFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceImageBuildFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 7 月 31 日, 世界標準時間 23:29
- 編輯時間：世界標準時間 2022 年 3 月 4 日下午 17 時 5 分
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceLicenseManagementServiceRolePolicy

描述：啟用 AWS Marketplace 對授權管理所使用或管理的資源的存取 AWS 服務 和資源。

`AWSMarketplaceLicenseManagementServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 12 月 3 日, 08:33 世界標準時間
- 編輯時間:2020 年十二月三日, 08:33 世界標準時間
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceManageSubscriptions

描述：提供訂閱和取消訂閱 AWS Marketplace 軟體的功能

AWSMarketplaceManageSubscriptions是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceManageSubscriptions至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2023 年 1 月 19 日 23:45
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceMeteringFullAccess

描述：提供對 AWS Marketplace 計量的完整存取權。

AWSMarketplaceMeteringFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceMeteringFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2016 年 3 月 17 日, 22:39
- 編輯時間：2016 年 3 月 17 日，世界標準時間 22:39
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceMeteringRegisterUsage

說明：提供透過 AWS Marketplace 計量服務註冊資源和追蹤使用情況的權限。

`AWSMarketplaceMeteringRegisterUsage`是AWS 受管理的策略。

使用此政策

您可以附加`AWSMarketplaceMeteringRegisterUsage`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月二十一日, 01:17 世界標
- 編輯時間:二零一九年十一月二十一日, 01:17 世界標
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceProcurementSystemAdminFullAccess

描述：提供 AWS Marketplace 電子採購整合之所有管理動作的完整存取權。

AWSMarketplaceProcurementSystemAdminFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceProcurementSystemAdminFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 25 日, 世界標準時間 13:07
- 編輯時間:2019 年 6 月 25 日, 世界標準時間 13:07
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplacePurchaseOrdersServiceRolePolicy

描述：啟用對採購單管理 AWS Marketplace 服務的存取。

`AWSMarketplacePurchaseOrdersServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 10 月 27 日, 世界標準時間 15:12
- 編輯時間:2021 年 10 月 27 日, 世界標準時間 15:12
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceRead-only

描述：提供檢 AWS Marketplace 閱訂閱的功能

AWSMarketplaceRead-only是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceRead-only至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2023 年 1 月 19 日晚上 23 點 30 分

- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceResaleAuthorizationServiceRolePolicy

描述：啟用「轉售授權」所使用或管理的存 AWS Marketplace 取權 AWS 服務 和資源。

AWSMarketplaceResaleAuthorizationServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2024 年 3 月 5 日, 18:47
- 編輯時間：世界標準時間 2024 年 3 月 5 日下午 18:47

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceSellerFullAccess

描述：提供對 AMI 管理等其他 AWS 服務的 AWS Marketplace 所有賣家操作的完全訪問權限。

AWSMarketplaceSellerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceSellerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 7 月 2 日, 世界標準時間 20:40

- **編輯時間**：世界標準時間 2024 年 3 月 15 日，16:09
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceSellerProductsFullAccess

描述：為賣家提供「AWS Marketplace 管理產品」頁面和其他 AWS 服務（例如 AMI 管理）的完整存取權。

AWSMarketplaceSellerProductsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceSellerProductsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 7 月 2 日, 世界標準時間 21:06
- 編輯時間：世界標準時間 2023 年 7 月 18 日 22:19
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMarketplaceSellerProductsReadOnly

說明：為賣家提供「AWS Marketplace 管理產品」頁面的唯讀存取權。

AWSMarketplaceSellerProductsReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSMarketplaceSellerProductsReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 7 月 2 日, 世界標準時間 21:40
- 編輯時間：2022 年十一月十九日，世界標準時間 00:08
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMediaConnectServicePolicy

描述：啟用存取權限的預設原則，以 AWS 服務 及使用或管理的資源 MediaConnect。

AWSMediaConnectServicePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 4 月 3 日, 世界標準時間 22:11
- 編輯時間:世界標準時間 2023 年 4 月 3 日, 22:11
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMediaTailorServiceRolePolicy

描述：啟用存取使用或管理的 AWS 資源 MediaTailor

AWSMediaTailorServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2021 年 9 月 17 日, 世界標準時間 22:27
- 編輯時間：2021 年 9 月 17 日，世界標準時間 22：27
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubDiscoveryAccess

說明：政策 AWSMigrationHubService 允許代 AWSApplicationDiscoveryService 表客戶撥打電話。

AWSMigrationHubDiscoveryAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubDiscoveryAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2017 年 8 月 14 日, 世界標準時間 13:30
- 編輯時間:2020 年 8 月 6 日, 世界標準時間 17:34
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubDMSAccess

說明：資 Database Migration Service 在客戶帳戶中扮演角色以呼叫 Migration Hub 的原則

AWSMigrationHubDMSAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubDMSAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 8 月 14 日, 世界標準時間下午 2 點
- 編輯時間：2019 年 10 月 7 日，世界標準時間 17:51
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubFullAccess

描述：提供客戶存取 Migration Hub 服務的受管理原則

AWSMigrationHubFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 8 月 14 日, 世界標準時間 14:02
- 編輯時間：2019 年 6 月 19 日，世界標準時間 21:14
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubFullAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubOrchestratorConsoleFullAccess

說明：提供對 AWS Migration Hub、 AWS 應用程式探索服務、Amazon 簡單儲存服務和 AWS Secrets Manager 的有限存取權限。此原則也會授與 AWS Migration Hub 協調器服務的完整存取權。

`AWSMigrationHubOrchestratorConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSMigrationHubOrchestratorConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 4 月 20 日，下午 2 時 26 分
- 編輯時間：世界標準時間 2023 年 12 月 5 日下午 17 時 34 分

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

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHO",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3MHO",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Configuration",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations",
        "discovery:GetDiscoverySummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetHomeRegion",
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
```

```
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListProfileRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Account",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-orchestrator.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
orchestrator.amazonaws.com/AWSServiceRoleForMigrationHubOrchestrator*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubOrchestratorInstanceRolePolicy

說明：我們的服務需要為 SAP 和 MGN 遷移執行個體附加此政策，以便從 S3 下載指令碼以協調執行個體，並擷取 EC2 執行個體內的機密值。

AWSMigrationHubOrchestratorInstanceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubOrchestratorInstanceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 4 月 20 日，下午 2 時 43 分
- 編輯時間:世界標準時間四月二十日, 2022 年 4 月 20 日
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubOrchestratorPlugin

描述：為 AWS 遷移中心協調器提供對 Amazon 簡單儲存服務、 AWS Secrets Manager 員和外掛程式相關動作的有限存取權。

AWSMigrationHubOrchestratorPlugin是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubOrchestratorPlugin至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 4 月 20 日，下午 2 時 25 分
- 編輯時間：世界標準時間：2022 年 4 月 20 日，02:25
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubOrchestratorServiceRolePolicy

說明：提供 Migration Hub 協調器所需的權限，以移轉及現代化您的內部部署工作負載

AWSMigrationHubOrchestratorServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 4 月 20 日，2022 年 2 月 24 日
- 編輯時間：世界標準時間 2024 年 3 月 4 日下午 18:25
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

說明：授予對 AWS Migration Hub 重構空間和其他 AWS 相關服務的完整存取權，但在使用沒有網路橋接器的環境時不需要 AWS Transit Gateway 和 EC2 安全群組除外。此政策也會排除 AWS Lambda 和 AWS Resource Access Manager 所需的許可，因為它們可以根據標籤設定範圍。

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 3 日, 世界標準時間 20:09
- 編輯時間:世界標準時間 2024 年 4 月 11 日, 18:16
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

描述：用於傳遞至 SSM 自動化文件的 IAM 服務角色 AWSRefactorSpaces-CreateResources 授與執行自動化所需的權限。該政策授予 EC2 標籤的讀取/寫入存取權，以追蹤自動化進度。啟用重構

Spaces 環境的網路橋接後，自動化也會將環境的安全群組新增至 EC2 執行個體，以允許來自環境中其他重構空間服務的流量。此原則也會授與應用程式移轉服務的啟動後動作 SSM 參數的存取權。

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubRefactorSpaces-SSMAutomationPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2023 年 8 月 10 日, 世界標準時間 15:08
- 編輯時間:世界標準時間 2023 年 8 月 10 日, 15:08
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubRefactorSpacesFullAccess

描述：授予對 AWS MigrationHub 重構空間、 AWS MigrationHub 重構空間主控台功能和其他相關 AWS 服務的完整存取權，但 AWS Lambda 和 AWS Resource Access Manager 所需的權限除外，因為它們可以根據標籤設定範圍。

AWSMigrationHubRefactorSpacesFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubRefactorSpacesFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二一年十一月二十九日, 07:12 世界標
- 編輯時間：世界標準時間 2024 年 4 月 11 日 17:45
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubRefactorSpacesServiceRolePolicy

描述：提供存取由 AWS Migration Hub 重構空間所管理或使用的 AWS 資源。

`AWSMigrationHubRefactorSpacesServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:11 月 29 日, 06:50 世界標準時間
- 編輯時間：世界標準時間 2023 年 7 月 20 日下午 15:57
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubSMSAccess

說明：伺服器移轉服務在客戶帳戶中扮演角色以呼叫 Migration Hub 的政策

AWSMigrationHubSMSAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubSMSAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 8 月 14 日, 世界標準時間 13:57
- 編輯時間:2019 年 10 月 7 日, 世界標準時間 18:01
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubStrategyCollector

說明：授予許可以允許與 AWS Migration Hub 策略建議服務通訊、與服務相關的 S3 儲存貯體的讀取/寫入存取權、Amazon API Gateway 存取上傳日誌和指標 AWS、 AWS Secrets Manager 以擷取登入資料的存取權，以及任何相關服務。

AWSMigrationHubStrategyCollector是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubStrategyCollector至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 10 月 19 日, 世界標準時間 20:15
- 編輯時間:世界標準時間 2024 年 4 月 1 日, 16:21
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubStrategyConsoleFullAccess

說明：授與「 AWS Migration Hub 策略建議」服務的完整存取權，以及透過 AWS Management Console. AWS

AWSMigrationHubStrategyConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMigrationHubStrategyConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 10 月 19 日, 世界標準時間 20:13
- 編輯時間:2022 年 11 月 9 日, 世界標準時間凌晨 00
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMigrationHubStrategyServiceRolePolicy

描述：啟用存取「AWS Migration Hub 策略建議」服務所使用或管理的 AWS 資源。

`AWSMigrationHubStrategyServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 10 月 19 日, 世界標準時間 20:02
- 編輯時間：2021 年 10 月 19 日，世界標準時間 20:02
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMobileHub_FullAccess

描述：此原則可附加至任何使用者、角色或群組，以便授與使用者在 AWS Mobile Hub 中建立、刪除及修改專案 (及其相關聯 AWS 資源) 的權限。這也包括產生和下載每個 Mobile Hub 專案範例行動應用程式原始程式碼的權限。

AWSMobileHub_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSMobileHub_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年一月 5 日, 世界標準時間 19:56
- 編輯時間：2019 年十二月十九日，世界標準時間 23:15
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
```

```
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMobileHub_ReadOnly

描述：此原則可附加至任何使用者、角色或群組，以便授與使用者在 AWS Mobile Hub 中列出及檢視專案的權限。這也包括產生和下載每個 Mobile Hub 專案範例行動應用程式原始程式碼的權限。它不允許使用者修改任何 Mobile Hub 專案的任何設定。

AWSMobileHub_ReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSMobileHub_ReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年一月 5 日, 世界標準時間 19:55
- 編輯時間:2018 年 7 月 23 日, 世界標準時間 21:59

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

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSMSKReplicatorExecutionRole

說明：授予 Amazon MSK 複寫器的許可，以便在 MSK 叢集之間複寫資料。

AWSMSKReplicatorExecutionRole是AWS 受管理的策略。

使用此政策

您可以附加AWSMSKReplicatorExecutionRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間：2023 年 12 月 6 日，00:07
- 編輯時間：世界標準時間 2024 年 3 月 25 日晚上 9 時 36 分
- ARN: arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSNetworkFirewallServiceRolePolicy

描述：允許 AWSNetworkFirewall 為防火牆創建和管理必要的資源。

AWSNetworkFirewallServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年十一月十七日, 世界標準時間 17:17
- 編輯時間：世界標準時間 2023 年 3 月 30 日下午 17 時 19 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSNetworkManagerCloudWANServiceRolePolicy

說明：允許存 NetworkManager 取與核心網路相關聯的資源

AWSNetworkManagerCloudWANServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 7 月 12 日，下午 12:17
- 編輯時間：世界標準時間 7 月 12 日，下午 12 時 17 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
```

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSNetworkManagerFullAccess

描述：提供完全訪問 Amazon NetworkManager 通過 AWS Management Console.

AWSNetworkManagerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSNetworkManagerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 17 世界標準時間
- 編輯時間:二零一九年十二月三日, 17 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSNetworkManagerReadOnlyAccess

說明：提供 NetworkManager 透過 Amazon 的唯讀存取權限 AWS Management Console。

AWSNetworkManagerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSNetworkManagerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月三日, 17:35 世界標準時
- 編輯時間：2019 年 12 月 3 日，世界標準時間 17:35
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSNetworkManagerServiceRolePolicy

說明：允許存 NetworkManager 取與全球網路相關聯的資源

AWSNetworkManagerServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十二月三日, 世界標準時間 14:
- 編輯時間：2022 年 7 月 27 日，世界標準時間 19:41
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOpsWorks_FullAccess

描述：提供對的完整存取權 AWS OpsWorks。

AWSOpsWorks_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSOpsWorks_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2021 年 1 月 22 日, 16:29
- 編輯時間:2021 年 1 月 22 日, 世界標準時間 16:29
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOpsWorksCloudWatchLogs

說明：啟用已啟用 CWLogs 整合的 OpsWorks 執行個體，以傳送記錄檔並建立必要的記錄群組

AWSOpsWorksCloudWatchLogs是AWS 受管理的策略。

使用此政策

您可以附加AWSOpsWorksCloudWatchLogs至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 3 月 30 日, 世界標準時間 17:47
- 編輯時間：2017 年 3 月 30 日，世界標準時間 17:47
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOpsWorksCMInstanceProfileRole

說明：為 OpsWorks CM 啟動的執行個體提供 S3 存取權。

AWSOpsWorksCMInstanceProfileRole是AWS 受管理的策略。

使用此政策

您可以附加AWSOpsWorksCMInstanceProfileRole至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:十一月二十四日, 09:48 世界標準時間
- 編輯時間：2021 年 4 月 23 日，世界標準時間 17：34
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOpsWorksCMServiceRole

描述：用於建立 OpsWorks CM 伺服器的服務角色原則。

AWSOpsWorksCMServiceRole是AWS 受管理的策略。

使用此政策

您可以附加AWSOpsWorksCMServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:十一月二十四日, 09:49 世界標準時間

- 編輯時間：2021 年 4 月 23 日，世界標準時間 17：32
- ARN: arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOpsWorksInstanceRegistration

說明：提供 Amazon EC2 執行個體的存取權，以便在 AWS OpsWorks 堆疊中註冊。

AWSOpsWorksInstanceRegistration是AWS 受管理的策略。

使用此政策

您可以附加AWSOpsWorksInstanceRegistration至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2016 年 6 月 3 日，世界標準時間 14:23
- 編輯時間：2016 年 6 月 3 日，世界標準時間 14:23
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOpsWorksRegisterCLI_EC2

說明：啟用透過 OpsWorks CLI 註冊 EC2 執行個體的政策

AWSOpsWorksRegisterCLI_EC2是AWS 受管理的策略。

使用此政策

您可以附加AWSOpsWorksRegisterCLI_EC2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 18 日, 世界標準時間 15:56
- 編輯時間：2019 年 6 月 18 日，世界標準時間 15:56
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOpsWorksRegisterCLI_OnPremises

說明：啟用透過 OpsWorks CLI 註冊內部部署執行個體的原則

AWSOpsWorksRegisterCLI_OnPremises是AWS 受管理的策略。

使用此政策

您可以附加AWSOpsWorksRegisterCLI_OnPremises至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 18 日, 世界標準時間 15:33
- 編輯時間：2019 年 6 月 18 日，世界標準時間 15:33
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOrganizationsFullAccess

描述：提供「Organ AWS izations」的完整存取權。

AWSOrganizationsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSOrganizationsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 11 月 6 日, 世界標準時間 20:31
- 編輯時間：世界標準時間 2024 年 2 月 6 日下午 17 時 49 分
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOrganizationsReadOnlyAccess

描述：提供「Organ AWS izations」的唯讀存取權。

AWSOrganizationsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSOrganizationsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 11 月 6 日, 世界標準時間 20:32

- **編輯時間**：世界標準時間 2024 年 2 月 6 日 17:36
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOrganizationsServiceTrustPolicy

描述：允許組 Organizations 與其他核准的組 AWS 織共用信任 AWS 服務 的政策，以簡化客戶組態。

AWSOrganizationsServiceTrustPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 10 月 10 日, 世界標準時間 23:04
- 編輯時間:2017 年 11 月 1 日, 06:01 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOutpostsAuthorizeServerPolicy

說明：此原則授與權限，允許您在內部部署網路上安裝 Outpost 伺服器。

AWSOutpostsAuthorizeServerPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSOutpostsAuthorizeServerPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 1 月 4 日, 世界標準時間 19:23
- 編輯時間:2023 年 1 月 4 日, 世界標準時間 19:23
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSOutpostsServiceRolePolicy

描述：服務連結角色原則，可讓您存取由 AWS Outposts 管理的 AWS 資源

AWSOutpostsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2020 年十一月九日, 世界標準時間 22:55
- 編輯時間：2020 年 11 月 9 日，世界標準時間 22:55
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPanoramaApplianceRolePolicy

描述：允許 AWS Panorama 設備上的 AWS IoT 軟體將日誌上傳到 Amazon CloudWatch。

AWSPanoramaApplianceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSPanoramaApplianceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 12 月 1 日, 13:13 世界標準時間
- 編輯時間:2020 年十二月 1 日, 13:13 世界標準時間
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPanoramaApplianceServiceRolePolicy

描述：允許 AWS Panorama 設備將日誌上傳到亞馬遜 CloudWatch，並從為與 Pan AWS orama 搭配使用而建立的 Amazon S3 存取點取得物件。

AWSPanoramaApplianceServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSPanoramaApplianceServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 10 月 20 日, 12:14
- 編輯時間：世界標準時間 2023 年 1 月 17 日 21:32
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPanoramaFullAccess

描述：提供對 AWS Panorama 的完整存取權

AWSPanoramaFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSPanoramaFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**:2020 年 12 月 1 日, 下午 13:12 世界標準時間
- **編輯時間**：世界標準時間 2022 年 1 月 12 日晚上 21 點 21 分
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPanoramaGreengrassGroupRolePolicy

說明：允許 AWS Panorama 設備上的 AWS Lambda 函數管理 Panorama 資源、將日誌和指標上傳到 Amazon CloudWatch，以及管理為與 Panorama 搭配使用而建立的值區中的物件。

AWSPanoramaGreengrassGroupRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSPanoramaGreengrassGroupRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 12 月 1 日, 下午 13:10 世界標準時間
- 編輯時間：世界標準時間 2021 年 1 月 6 日 19:30
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPanoramaSageMakerRolePolicy

描述：允許 Amazon 管理創建 SageMaker 用於與 AWS Panorama 一起使用的存儲桶中的對象。

AWSPanoramaSageMakerRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSPanoramaSageMakerRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 12 月 1 日, 13:13 世界標準時間
- 編輯時間:2020 年十二月 1 日, 13:13 世界標準時間
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

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

```
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPanoramaServiceLinkedRolePolicy

描述：允許 AWS Panorama 管理 AWS IoT， AWS Secrets Manager 和 AWS Panorama 資源。

AWSPanoramaServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 10 月 20 日, 12:12
- 編輯時間：2021 年十月二十日，世界標準時間 12:12
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPanoramaServiceRolePolicy

描述：允許 AWS Panorama 管理 Amazon S3、 AWS IoT、 AWS IoT、 AWS Lambda GreenGrass SageMaker、Amazon 和 Amazon CloudWatch 日誌中的資源，並將服務角色傳遞到 AWS AWS IoT GreenGrass、IoT 和 Amazon SageMaker。

AWSPanoramaServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSPanoramaServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 12 月 1 日, 下午 13:14 世界標準時間
- 編輯時間：2020 年 12 月 1 日，世界標準時間 13:14
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
```

```
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
```

```
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*",
        "panorama:Get*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
```

```
    {
      "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassIoTRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PanoramaGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteResourceDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
```

```
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaLambdaUsersFunctionAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:StopCompilationJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/panorama*",
        "arn:aws:sagemaker:*:*:compilation-job/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCompilationJobs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
```

```
      ]
    },
    {
      "Sid" : "PanoramaCWLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:CreateRoleAlias"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*",
        "arn:aws:iot:*:*:rolealias/panorama*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPriceListServiceFullAccess

摘要：提供「AWS 價目表服務」的完整存取權。

AWSPriceListServiceFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSPriceListServiceFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月二十二日，世界標準時間 00:36

- 編輯時間：2017 年十一月二十二日，世界標準時間 00:36
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "pricing:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPrivateCAAuditor

描述：提供稽核員存取 AWS 私有憑證授權單位

`AWSPrivateCAAuditor`是AWS 受管理的策略。

使用此政策

您可以附加AWSPrivateCAAuditor至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 2 月 14 日, 18:33
- 編輯時間：世界標準時間 2023 年 2 月 14 日下午 18:33
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAAuditor

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPrivateCAFullAccess

描述：提供 AWS 私有憑證授權單位的完整存取權

AWSPrivateCAFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSPrivateCAFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 2 月 14 日, 18:20
- 編輯時間：世界標準時間 2023 年 2 月 14 日下午 18:20
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPrivateCAPrivilegedUser

說明：提供有權限的憑證使用者存取 AWS 私人憑證授權機

AWSPrivateCAPrivilegedUser是AWS 受管理的策略。

使用此政策

您可以附加AWSPrivateCAPrivilegedUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 2 月 14 日, 18:26
- 編輯時間：世界標準時間 2023 年 2 月 14 日下午 18:26
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPrivateCAReadOnly

描述：提供 AWS 私人憑證授權單位的唯讀存取權

AWSPrivateCAReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSPrivateCAReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 2 月 14 日下午 6 時 30 分
- 編輯時間：世界標準時間 2023 年 2 月 14 日下午 6 時 30 分
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAReadOnly

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
  }
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPrivateCAUser

描述：提供憑證使用者存取 AWS 私人憑證授權單位

AWSPrivateCAUser是AWS 受管理的策略。

使用此政策

您可以附加AWSPrivateCAUser至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 2 月 14 日, 18:16
- 編輯時間：世界標準時間 2023 年 2 月 14 日下午 18:16
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAUser

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPrivateMarketplaceAdminFullAccess

描述：提供 AWS 私人 Marketplace 所有管理動作的完整存取權。

AWSPrivateMarketplaceAdminFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSPrivateMarketplaceAdminFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十七日, 世界標準時間 16:32
- 編輯時間：世界標準時間 2024 年 2 月 14 日 22:05
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPrivateMarketplaceRequests

描述：提供在 AWS 私人 Marketplace 中建立請求的存取權。

AWSPrivateMarketplaceRequests是AWS 受管理的策略。

使用此政策

您可以附加AWSPrivateMarketplaceRequests至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十月 28 日, 世界標準時間 21:44
- 編輯時間：2019 年 10 月 28 日，世界標準時間 21:44
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
```

```
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPrivateNetworksServiceRolePolicy

描述：允許 AWS 私人網路服務代表客戶管理資源。

AWSPrivateNetworksServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間:2021 年十二月十六日, 23:17
- 編輯時間：2021 年十二月十六日，世界標準時間 23:17
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSProtonCodeBuildProvisioningBasicAccess

說明：權限 CodeBuild 必須執行 AWS Proton CodeBuild 佈建的組建。

AWSProtonCodeBuildProvisioningBasicAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSProtonCodeBuildProvisioningBasicAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：二零二二年十一月九日晚

- 編輯時間：二零二二年十一月九日，世界標準時間晚
- ARN: arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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:*:*:*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSProtonCodeBuildProvisioningServiceRolePolicy

說明：允許 AWS Proton 代表您使用 CodeBuild 和其他 AWS 服務來管理 Proton 資源佈建。

AWSProtonCodeBuildProvisioningServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：二零二二年十一月九日晚
- 編輯時間:2023 年 5 月 17 日, 世界標準時間 16:11
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSProtonDeveloperAccess

說明：提供對 AWS Proton API 和管理主控台的存取權，但不允許管理 Proton 範本或環境。

AWSProtonDeveloperAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSProtonDeveloperAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 2 月 17 日, 世界標準時間 19:02
- 編輯時間：2022 年十一月十八日，世界標準時間 18:35
- ARN: arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
```

```
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
```

```
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSProtonFullAccess

說明：提供對 AWS Proton API 和管理主控台的完整存取權。除了這些許可之外，還需要存取 Amazon S3 才能從 S3 儲存貯體註冊範本服務包，以及存取 Amazon IAM 以建立和管理 Proton 的服務角色。

`AWSProtonFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSProtonFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2021 年 2 月 17 日，世界標準時間 19:07
- 編輯時間：世界標準時間 6 月 20 日，2022 年 12 月 36 日
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sync.proton.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:PassConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSProtonReadOnlyAccess

說明：提供 AWS Proton API 和管理主控台的唯讀存取權。

AWSProtonReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSProtonReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 2 月 17 日, 世界標準時間 19:09
- 編輯時間：2022 年十一月十八日，世界標準時間 18:28
- ARN: arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
```

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSProtonServiceGitSyncServiceRolePolicy

說明：允許 AWS Proton 將您的服務、環境和元件定義從 Git 儲存庫同步到 AWS Proton 的政策。

`AWSProtonServiceGitSyncServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 4 月 4 日, 世界標準時間下午 3:55
- 編輯時間：世界標準時間 2023 年 4 月 4 日，下午 3:55
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSProtonSyncServiceRolePolicy

說明：允許 AWS Proton 將您的 git 存儲庫內容同步到質子或將質子內容同步到您的 git 存儲庫的策略。

AWSProtonSyncServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年十一月二十三日, 世界標準時間 21:14
- 編輯時間：2024 年 5 月 5 日凌時 49 分世界標準時間
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSPurchaseOrdersServiceRolePolicy

說明：授與在帳單主控台上檢視和修改採購單的權限

AWSPurchaseOrdersServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSPurchaseOrdersServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 6 日, 世界標準時間 18:15
- 編輯時間：世界標準時間 2023 年 7 月 17 日 18:59
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightAssetBundleExportPolicy

描述：提供執行 QuickSight 資產包匯出作業所需的權限集

`AWSQuickSightAssetBundleExportPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`AWSQuickSightAssetBundleExportPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2024 年 3 月 27 日 21:31
- 編輯時間：世界標準時間 2024 年 3 月 27 日 21:31
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:ListRefreshSchedules",
        "quicksight:DescribeDataSetPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
```

```
      "Sid" : "DataSourceReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "VPCConnectionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeVPCConnection",
        "quicksight:ListVPCConnections"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "RefreshScheduleReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "AssetBundleExportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleExportJob",
        "quicksight:ListAssetBundleExportJobs",
        "quicksight:StartAssetBundleExportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-export-job/*"
    }
```

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightAssetBundleImportPolicy

描述：提供執行 QuickSight 資產套件匯入作業所需的權限集

AWSQuickSightAssetBundleImportPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSQuickSightAssetBundleImportPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2024 年 3 月 27 日 21:40
- 編輯時間：世界標準時間 2024 年 3 月 27 日 21:40
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "TagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource",
        "quicksight:TagResource",
        "quicksight:UntagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDashboard",
        "quicksight:DeleteDashboard",
        "quicksight:DescribeDashboard",
        "quicksight:UpdateDashboard",
        "quicksight:UpdateDashboardPublishedVersion",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:UpdateDashboardPermissions",
        "quicksight:UpdateDashboardLinks"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateAnalysis",
        "quicksight:DeleteAnalysis",
        "quicksight:DescribeAnalysis",
        "quicksight:UpdateAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:UpdateAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
```

```
        "quicksight:DeleteDataSet",
        "quicksight:DescribeDataSet",
        "quicksight:PassDataSet",
        "quicksight:UpdateDataSet",
        "quicksight:DeleteDataSetRefreshProperties",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:PutDataSetRefreshProperties",
        "quicksight:UpdateDataSetPermissions",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:ListRefreshSchedules"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:DescribeDataSource",
        "quicksight:DeleteDataSource",
        "quicksight:PassDataSource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateTheme",
        "quicksight:DeleteTheme",
        "quicksight:DescribeTheme",
        "quicksight:UpdateTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:UpdateThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "RefreshScheduleWriteAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "quicksight:CreateRefreshSchedule",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DeleteRefreshSchedule",
        "quicksight:UpdateRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "VPCConnectionWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListVPCConnections",
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "AssetBundleImportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleImportJob",
        "quicksight:ListAssetBundleImportJobs",
        "quicksight:StartAssetBundleImportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuicksightAthenaAccess

說明：快速查詢存取用於 Athena 查詢結果的 Athena API 和 S3 儲存貯體

AWSQuicksightAthenaAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSQuicksightAthenaAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：二零一六年十二月九日，02:31 世界標準時
- 編輯時間:2021 年 7 月 7 日, 世界標準時間 20:09
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
```

```
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
```

```
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightDescribeRDS

說明：允 QuickSight 許描述 RDS 資源

AWSQuickSightDescribeRDS是AWS 受管理的策略。

使用此政策

您可以附加AWSQuickSightDescribeRDS至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:十一月十日, 世界標準時間 23:24
- 編輯時間：2015 年 11 月 10 日，世界標準時間 23:24
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightDescribeRedshift

描述：允許描述 Redshift QuickSight 資源

AWSQuickSightDescribeRedshift是AWS 受管理的策略。

使用此政策

您可以附加AWSQuickSightDescribeRedshift至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一五年十一月十日 23:25 世界標準時間
- 編輯時間:2015 年 11 月 10 日, 世界標準時間 23:25
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "redshift:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightElasticsearchPolicy

說明：提供從 Amazon 對 Amazon 彈性搜索資源的訪問 QuickSight

AWSQuickSightElasticsearchPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSQuickSightElasticsearchPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 9 月 9 日, 世界標準時間 17:27
- 編輯時間：2021 年 9 月 7 日，世界標準時間 23:25
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
```

```
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightIoTAnalyticsAccess

說明：提供 IoT Analytics 資料集的 QuickSight 唯讀存取權

`AWSQuickSightIoTAnalyticsAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSQuickSightIoTAnalyticsAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年 11 月 29 日，世界標準時間下午 5:00
- 編輯時間：2017 年 11 月 29 日，世界標準時間 17:00
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iotanalytics:ListDatasets",
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightListIAM

說明：允 QuickSight 許列出 IAM 實體

AWSQuickSightListIAM是AWS 受管理的策略。

使用此政策

您可以附加AWSQuickSightListIAM至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零一五年十一月十日 23:25 世界標準時間

- 編輯時間:2015 年 11 月 10 日, 世界標準時間 23:25
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuicksightOpenSearchPolicy

說明：提供從 Amazon 訪問 Amazon OpenSearch 資源 QuickSight

`AWSQuicksightOpenSearchPolicy`是AWS 受管理的策略。

使用此政策

您可以附加AWSQuicksightOpenSearchPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2021 年 9 月 7 日, 世界標準時間 23:26
- 編輯時間：2021 年 9 月 7 日，世界標準時間 23:26
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightSageMakerPolicy

說明：提供從 Amazon 訪問 Amazon SageMaker 資源 QuickSight

AWSQuickSightSageMakerPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSQuickSightSageMakerPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 1 月 17 日, 世界標準時間 17:18
- 編輯時間：世界標準時間 2023 年 10 月 30 日下午 17 時 57 分
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSQuickSightTimestreamPolicy

說明： AWS QuickSight 存取時 AWS 間串流 API。客戶可以將此原則附加至 AWS QuickSight 角色，以便擷取資料和中繼資料。

AWSQuickSightTimestreamPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSQuickSightTimestreamPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 9 月 30 日, 世界標準時間 21:47
- 編輯時間：2020 年 9 月 30 日，世界標準時間 21:47
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSReachabilityAnalyzerServiceRolePolicy

描述：允許 VPC 可 Reachability Analyzer 代表您存取 AWS 資源並與 Organ AWS izations 整合。

`AWSReachabilityAnalyzerServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：二零二年十一月二十三日
- 編輯時間：2024 年 5 月 15 日，世界標準時間 20:49
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
```

```
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSRefactoringToolkitFullAccess

描述：此原則授與使用 AWS 具組的 .NET 重構延伸模組 AWS 服務的權限。它旨在附加到本地配 AWS 置文件。該政策允許上傳應用程式成品，並從 Amazon S3 下載產生的成品。它允許使用亞馬遜彈性容器註冊表（Amazon ECR）存儲 AWS CodeBuild 和檢索映像將應用程序構建到容器映像中。它允許將應用程式部署到容器服務， AWS 例如 Amazon Elastic Container Service (Amazon ECS)、選擇性建立 VPC 資源、與現有基礎設施 (例如 AWS Directory Service) 的選擇性連線，以及其他相關服務。

AWSRefactoringToolkitFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSRefactoringToolkitFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：2022 年 10 月 25 日，16:41
- 編輯時間：世界標準時間 2024 年 3 月 25 日下午 18:43
- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSRefactoringToolkitSidecarPolicy

描述：此原則適用於 AWS 使用 Microsoft Visual Studio 的 .NET 重構延伸模 AWS 組中為測試應用程式而建立的 Amazon ECS 任務。該政策授予從 Amazon S3 下載應用程式成品的存取權、使用 AWS Systems Manager 傳達任務狀態，以及其他必要服務。

AWSRefactoringToolkitSidecarPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSRefactoringToolkitSidecarPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**：世界標準時間：2022 年 10 月 25 日，16:41
- **編輯時間**：2022 年十月二十九日，世界標準時間 22:15
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSrePostPrivateCloudWatchAccess

說明：提供 Re: 私人貼文存取權以發佈 CloudWatch 測量結果資料

`AWSrePostPrivateCloudWatchAccess`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 15 日，16:37
- 編輯時間：世界標準時間 2023 年 11 月 15 日，16:37
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPublishMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/rePostPrivate",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSRepostSpaceSupportOperationsPolicy

描述：此原則允許 Re: POST Space 服務建立、管理及解決透過 Space 應用程式建立的 Support 案例。

AWSRepostSpaceSupportOperationsPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSRepostSpaceSupportOperationsPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間:2023 年 11 月 26 日, 21:52
- 編輯時間：世界標準時間 2023 年 11 月 26 日晚上 9 時 52 分
- ARN: arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResilienceHubAsssessmentExecutionPolicy

說明： AWS 復原中樞服務角色的原則，允許存取其他 AWS 服務以執行評估。

AWSResilienceHubAsssessmentExecutionPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSResilienceHubAsssessmentExecutionPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 6 月 27 日
- 編輯時間：世界標準時間 2024 年 3 月 24 日下午 18:05
- ARN: arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceAccessManagerFullAccess

描述：提供 AWS Resource Access Manager 的完整存取權

AWSResourceAccessManagerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSResourceAccessManagerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 4 日, 世界標準時間 17:28
- 編輯時間:2019 年 6 月 4 日, 世界標準時間 17:28
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:*"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceAccessManagerReadOnlyAccess

描述：提供 AWS Resource Access Manager 的唯讀存取權。

AWSResourceAccessManagerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSResourceAccessManagerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 12 月 9 日, 世界標準時間 20:58
- 編輯時間：2019 年 12 月 9 日，世界標準時間 20:58
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceAccessManagerResourceShareParticipantAccess

描述：可讓您存取 AWS 資源共用參與者所需的 Resource Access Manager API。

AWSResourceAccessManagerResourceShareParticipantAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSResourceAccessManagerResourceShareParticipantAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月九日, 世界時間 20:41

- **編輯時間**：2019 年 12 月 9 日，世界標準時間 20:41
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceAccessManagerServiceRolePolicy

描述：包含客戶 Organizations 結構之唯讀 AWS Resource Access Manager 存取權的原則。它也包含可以自行刪除角色的 IAM 許可。

AWSResourceAccessManagerServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月十四日, 世界標準時間 19:28
- 編輯時間：2018 年十一月十四日，世界標準時間 19:28
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceExplorerFullAccess

描述：此原則會授與存取 Resource Explorer 資源的系統管理權限，並將唯讀權限授與其他 AWS 服務以支援此存取。

`AWSResourceExplorerFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSResourceExplorerFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間**：二 ○ 二 ○ 二年十一月七日，世界標準時間
- **編輯時間**：世界標準時間：2023 年 11 月 14 日，下午 16:53
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceExplorerOrganizationsAccess

描述：此原則會授與資源總管的系統管理權限，並將唯讀權限授與其他 AWS 服務以支援此存取。Organ AWS izations 管理員需要這些權限，才能在主控台中設定和管理多帳戶搜尋。

`AWSResourceExplorerOrganizationsAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSResourceExplorerOrganizationsAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 11 月 14 日下午 17 時 01 分
- 編輯時間：世界標準時間 2023 年 11 月 14 日下午 17 時 01 分
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerGetSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    },
    {
      "Sid" : "ResourceExplorerCreateSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationsAdministratorAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceExplorerReadOnlyAccess

描述：此原則會授與唯讀權限，以搜尋及檢視 Resource Explorer 資源，並將唯讀權限授與其他 AWS 服務以支援此存取。

AWSResourceExplorerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSResourceExplorerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零二年十一月七日，世界標準時間 19:56
- 編輯時間:2023 年 11 月 14 日, 世界標準時間 16:43
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceExplorerServiceRolePolicy

描述：允許 Resource Explorer 代表您檢視資源和 CloudTrail 事件，以便為您的資源建立索引以進行搜尋。

`AWSResourceExplorerServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2022 年 10 月 25 日，世界標準時間 20:35
- 編輯時間：世界標準時間 2023 年 12 月 20 日，下午 13:58
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-explorer-2/*"
      ]
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/deployments"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "amplify:ListApps",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListThemes",
        "app-integrations:ListEventIntegrations",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appsync:ListGraphqlApis",
        "aps:ListRuleGroupsNamespaces",
```

```
        "aps:ListWorkspaces",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeguru-profiler:ListProfilingGroups",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "databrew:ListDatasets",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "detective:ListGraphs",
        "ds:DescribeDirectories",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
```

```
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpams",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTrafficMirrorFilters",
```

```
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSubnetCidrReservations",
        "ecr:DescribeRepositories",
        "ecr-public:DescribeRepositories",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "emr-serverless:ListApplications",
        "es:ListDomainNames",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:ListExperimentTemplates",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetLabels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "gamelift:ListAliases",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "greengrass:ListComponents",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetTables",
        "glue:GetTriggers",
        "greengrass:ListComponentVersions",
        "greengrass:ListGroups",
        "healthlake:ListFHIRDatastores",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
```

```
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iot:ListJobTemplates",
        "iot:ListAuthorizers",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListSecurityProfiles",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListWorkspaces",
        "kafka:ListConfigurations",
        "kms:ListKeys",
        "ivs:ListChannels",
        "ivs:ListStreamKeys",
        "kafka:ListClusters",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
```

```
        "kinesisvideo:ListStreams",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "lookoutmetrics:ListAlerts",
        "lookoutvision:ListProjects",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mq:ListBrokers",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "panorama:ListPackages",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "qldb:ListJournalKinesisStreamsForLedger",
```

```
        "qldb:ListLedgers",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroups",
```

```
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverRules",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListStorageLensConfigurations",
        "sagemaker:ListModels",
        "sagemaker:ListNotebookInstances",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm-incidents:ListResponsePlans",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListInventoryEntries",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "timestream:ListDatabases",
        "wisdom:listAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:listKnowledgeBases"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSResourceGroupsReadOnlyAccess

描述：這是 Res AWS ource Groups 的唯讀政策

`AWSResourceGroupsReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSResourceGroupsReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 7 日, 10:27 世界標準時間
- 編輯時間：2019 年 2 月 5 日，世界標準時間 17:56
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSRoboMaker_FullAccess

描述：提供 AWS RoboMaker 透過 AWS Management Console 和 SDK 的完整存取權。還提供對相關服務（例如 S3，IAM）的選擇訪問權限。

AWSRoboMaker_FullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSRoboMaker_FullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 9 月 10 日，世界標準時間 18:34
- 編輯時間：世界標準時間 2021 年 9 月 16 日晚上 9 時 6 分
- ARN: arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSRoboMakerReadOnlyAccess

說明：透 AWS RoboMaker 過 AWS Management Console 和 SDK 提供唯讀存取權

AWSRoboMakerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSRoboMakerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一八年十一月二十六日, 世界標準時
- 編輯時間:2020 年 8 月 28 日, 世界標準時間 23:10
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSRoboMakerServicePolicy

描述： RoboMaker 服務政策

AWSRoboMakerServicePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 11 月 26 日, 世界標準時間 06:30
- 編輯時間：2021 年十一月十一日，世界標準時間 22：23
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSRoboMakerServiceRolePolicy

描述： RoboMaker 服務政策

AWSRoboMakerServiceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSRoboMakerServiceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一八年十一月二十六日, 05:33 世界標
- 編輯時間:2018 年十一月二十六日, 05:33 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSRolesAnywhereServicePolicy

說明：允許 IAM 角色在任何地方發佈服務/使用指標， CloudWatch 並代表您檢查私有憑證授權單位的狀態。

AWSRolesAnywhereServicePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 7 月 5 日, 下午 3:26
- 編輯時間：世界標準時間：2022 年 7 月 5 日，下午 3:26
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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:*:*:*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSS3OnOutpostsServiceRolePolicy

說明：允許 Outposts 上的 Amazon S3 代表您管理 EC2 網路資源。

AWSS3OnOutpostsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間**:世界標準時間 2023 年 10 月 3 日, 20:32
- **編輯時間**：世界標準時間 2023 年 10 月 3 日晚上 20:32
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSavingsPlansFullAccess

描述：提供 Savings Plans 服務的完全訪問權限

AWSSavingsPlansFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSavingsPlansFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一九年十一月六日, 世界標準時間 22
- 編輯時間：2019 年 11 月 6 日，世界標準時間 22:45
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSavingsPlansReadOnlyAccess

說明：提供 Savings Plans 服務的唯讀權限

AWSSavingsPlansReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSavingsPlansReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一九年十一月六日, 世界標準時間 22
- 編輯時間：2019 年 11 月 6 日，世界標準時間 22:45
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
```

```
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSecurityHubFullAccess

描述：提供使用 AWS Security Hub 的完整存取權。

AWSSecurityHubFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSecurityHubFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十七日, 世界標準時間 23:54
- 編輯時間:世界標準時間 2024 年 4 月 23 日, 18:35
- ARN: arn:aws:iam::aws:policy/AWSSecurityHubFullAccess

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSecurityHubOrganizationsAccess

描述：授予在組織內啟用和管理 AWS Security Hub 的權限。包括在整個組織中啟用服務，以及決定服務的委派管理員帳戶。

AWSSecurityHubOrganizationsAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSecurityHubOrganizationsAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2021 年 3 月 15 日, 世界標準時間 20:53
- 編輯時間：世界標準時間 2023 年 11 月 16 日晚上 9 點 13 分
- ARN: arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSecurityHubReadOnlyAccess

說明：提供 AWS Security Hub 資源的唯讀存取權

AWSSecurityHubReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSecurityHubReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 11 月 28 日, 01:34 世界標準時間
- 編輯時間：世界標準時間 2024 年 2 月 22 日 23:45
- ARN: arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
```

```
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSecurityHubServiceRolePolicy

描述：資 AWS Security Hub 存取您的資源所需的服務連結角色。

AWSSecurityHubServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月二十七日, 世界標準時間 23:47
- 編輯時間:世界標準時間十一月二十七日, 下午 3 時 46 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy

政策版本

策略版本：v14(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogAdminFullAccess

描述：提供服務目錄管理功能的完整存取權

AWSServiceCatalogAdminFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSServiceCatalogAdminFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 2 月 15 日, 世界標準時間 17:19
- 編輯時間:世界標準時間 2023 年 4 月 13 日, 18:43
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogAdminReadOnlyAccess

描述：提供 Service Catalog 管理功能的唯讀存取權

AWSServiceCatalogAdminReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSServiceCatalogAdminReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 10 月 25 日, 18:53 世界標準時間
- 編輯時間:2019 年 10 月 25 日, 世界標準時間 18:53
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogAppRegistryFullAccess

描述：提供 Service Catalog 應用程式登錄功能的完整存取權

AWSServiceCatalogAppRegistryFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSServiceCatalogAppRegistryFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十一月十二日, 世界標準時間 22:25
- 編輯時間：世界標準時間 2023 年 12 月 7 日晚上 9 時 50 分
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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:*:*:*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogAppRegistryReadOnlyAccess

說明：提供 Service Catalog 應用程式登錄功能的唯讀存取權

AWSServiceCatalogAppRegistryReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSServiceCatalogAppRegistryReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十一月十二日, 世界標準時間 22:34
- 編輯時間：2022 年十一月十七日，世界標準時間 18:16
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogAppRegistryServiceRolePolicy

描述：允許 Service Catalog AppRegistry 代表您管理 Resource Groups

`AWSServiceCatalogAppRegistryServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 5 月 18 日, 世界標準時間 22:18
- 編輯時間：2022 年 10 月 26 日，世界標準時間 16:05
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
```

```
  "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*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogEndUserFullAccess

描述：提供服務目錄一般使用者功能的完整存取權

AWSServiceCatalogEndUserFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSServiceCatalogEndUserFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 2 月 15 日, 世界標準時間 17:22
- 編輯時間：2019 年 7 月 10 日，世界標準時間 20:30
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogEndUserReadOnlyAccess

描述：提供 Service Catalog 一般使用者功能的唯讀存取

AWSServiceCatalogEndUserReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSServiceCatalogEndUserReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 10 月 25 日, 18:49 世界標準時間
- 編輯時間:2019 年 10 月 25 日, 18:49 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

描述：要與組織組 Organ AWS izations 結構同步 AWS ServiceCatalog 的服務連結角色原則

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2023 年 4 月 10 日, 20:48
- 編輯時間：世界標準時間 2023 年 4 月 10 日，20:48

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceCatalogSyncServiceRolePolicy

說明：從來源儲存庫同步啟動設定人工因素的服務連結角色 AWS ServiceCatalog

AWSServiceCatalogSyncServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：二零二二年十一月十五日
- 編輯時間:世界標準時間 5 月 3 日, 下午 17 時 12 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForAmazonEKSNodegroup

說明：管理客戶帳戶中節點群組所需的權限。這些與管理下列資源相關的原則： AutoscalingGroups SecurityGroups、 LaunchTemplates 和 InstanceProfiles。

`AWSServiceRoleForAmazonEKSNodegroup`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月七日, 01:34 世界時間
- 編輯時間:2024 年 1 月 4 日, 世界標準時間 20:37
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForAmazonQDeveloper

說明：此服務連結角色可讓 Amazon Q 開發人員提供使用資訊。

AWSServiceRoleForAmazonQDeveloper是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 4 月 25 日，下午 7 時 40 分
- 編輯時間:2024 年 4 月 25 日, 07:40 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

描述：提供對 CloudWatch 警報使用的 Systems Manager 資源的存取

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 10 月 1 日, 09:49 世界標準時間
- 編輯時間:2020 年 10 月 1 日, 09:49 世界標準時間
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

說明：允 CloudWatch 許代表您存取 RDS Performance Insights 指標

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：2023 年 9 月 7 日，09:32
- 編輯時間：世界標準時間：2023 年 9 月 7 日，09:32
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForCodeGuru-Profiler

說明：Amazon CodeGuru 效能分析工具代表您傳送通知所需的服務連結角色。

AWSServiceRoleForCodeGuru-Profiler是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 6 月 26 日, 世界標準時間 22:04
- 編輯時間:2020 年 6 月 26 日, 世界標準時間 22:04
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForCodeWhispererPolicy

描述：此角色授予存取帳戶中資料的權限以計算帳單、提供在 Amazon 中建立和存取安全報告的存取權 CodeGuru，以及向 CloudWatch其發送資料。 CodeWhisperer

`AWSServiceRoleForCodeWhispererPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 3 月 24 日，19:39
- 編輯時間：世界標準時間 2024 年 3 月 29 日 22:13
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForEC2ScheduledInstances

說明：允許 EC2 排程執行個體啟動和管理競價型執行個體。

AWSServiceRoleForEC2ScheduledInstances是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 10 月 12 日, 世界標準時間 18:31
- 編輯時間:2017 年 10 月 12 日, 世界標準時間 18:31
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

說明： AWS GroundStation 使用此服務連結角色來叫用 EC2 尋找公用 IPv4 位址

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間：世界標準時間：2022 年十二月十三日 23:52**
- **編輯時間：2022 年十二月十三日，世界標準時間 23:52**
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForImageBuilder

說明：允許 EC2 ImageBuilder 代表您呼叫 AWS 服務。

`AWSServiceRoleForImageBuilder`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月二十九日, 世界標準時
- 編輯時間：世界標準時間 2023 年 10 月 19 日晚上 9 點 30 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

政策版本

策略版本：v19(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeAssociationExecutions",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:StartAutomationExecution",
      "Resource" : "arn:aws:ssm:*:*:automation-definition/ImageBuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
```

```
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForIoTSiteWise

描述：允許 AWS IoT SiteWise 佈建和管理閘道以及查詢資料。該政策包括部署到群組所需的 AWS Greengrass 權限、用於建立和更新服務前置詞函數的 AWS Lambda 許可，以及用於查詢資料存放區資料的 AWS IoT Analytics 權限。

`AWSServiceRoleForIoTSiteWise`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月十四日, 世界標準時間 19:19
- 編輯時間:2023 年 11 月 13 日, 世界標準時間 18:27
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
```

```
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForLogDeliveryPolicy

描述：允許記錄傳遞服務代表您呼叫記錄目的地，以傳遞記錄檔。

AWSServiceRoleForLogDeliveryPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十月四日, 17:31 世界標準時間
- 編輯時間:2021 年 7 月 15 日, 世界標準時間 20:07
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForMonitronPolicy

說明：授予 Amazon Monitron 許可以管理 AWS 資源，包括代表您進行 AWS SSO 使用者指派。

AWSServiceRoleForMonitronPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則

- **創建時間**:2020 年 12 月 2 日, 世界標準時間 19:06
- **編輯時間**：2022 年 9 月 29 日，世界標準時間 20:38
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForNeptuneGraphPolicy

說明：提供 Cloudwatch 存取權，以便為 Amazon Neptune 發佈操作和使用指標和日誌

AWSServiceRoleForNeptuneGraphPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 29 日，下午 3 點 3 分
- 編輯時間：世界標準時間十一月二十九日，下午 3 點 3 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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}"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForPrivateMarketplaceAdminPolicy

描述：提供描述和更新私人 Marketplace 資源和描述 Organ AWS izations 的權限

`AWSServiceRoleForPrivateMarketplaceAdminPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2024 年 2 月 14 日, 世界標準時間 22:28
- 編輯時間：世界標準時間 2024 年 2 月 14 日 22:28
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForSMS

說明：提供將 AWS AWS 服務執行個體遷移至 EC2、S3 和雲形所需的服務和資源的存取權。

AWSServiceRoleForSMS是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 8 月 6 日, 世界標準時間 18:39
- 編輯時間:2020 年 10 月 15 日, 世界標準時間 17:28
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

政策版本

策略版本：v10(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRoleForUserSubscriptions

描述：可讓您存取 Identity Center 資源的「使用者訂閱」服務，以自動更新您的訂閱。

AWSServiceRoleForUserSubscriptions是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 4 月 25 日, 世界標準時間 16:14
- 編輯時間:世界標準時間 2024 年 4 月 25 日, 16:14
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRolePolicyForBackupReports

說明：提供 AWS Backup 權限，以代表您建立符合性報告

AWSServiceRolePolicyForBackupReports是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 8 月 19 日, 世界標準時間 21:16
- 編輯時間：世界標準時間 2023 年 3 月 10 日凌時 51 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSServiceRolePolicyForBackupRestoreTesting

描述：此原則包含測試還原和清除測試期間建立之資源的權限。

AWSServiceRolePolicyForBackupRestoreTesting是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 10 日 23:37
- 編輯時間：世界標準時間 2024 年 2 月 14 日 22:42
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSShieldDRTAccessPolicy

說明：為 AWS DDoS 回應小組提供有限的存取權限， AWS 帳戶 以便在高嚴重性事件期間協助降低 DDoS 攻擊。

AWSShieldDRTAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSShieldDRTAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年 6 月 5 日, 世界標準時間 22:29
- 編輯時間:2020 年十二月十五日, 世界標準時間 17:28
- ARN: arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSShieldServiceRolePolicy

描述：允許 AWS Shield 代表您訪問 AWS 資源以提供 DDoS 保護。

AWSShieldServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零二一年十一月十七日, 世界標準時間
- 編輯時間：2021 年十一月十七日，世界標準時間 19:17
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSSMForSAPServiceLinkedRolePolicy

描述：為 SAP AWS Systems Manager 提供管理和整合 SAP 軟體所需的權限 AWS。

AWSSSMForSAPServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間十一月十六日（世界時間）
- 編輯時間:2024 年 4 月 11 日, 世界標準時間 18:31
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
```

```
    },
    {
      "Sid" : "InstanceTagActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
```

```
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:*:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
```

```
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
```

```
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    },
    {
      "Sid" : "StartStopInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSSMOpsInsightsServiceRolePolicy

描述：服務連結角色的原則 AWSServiceRoleForAmazonSSM_OpsInsights

AWSSSMOpsInsightsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 6 月 16 日, 世界標準時間 20:12
- 編輯時間：2021 年 6 月 16 日，世界標準時間 20:12
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSSODirectoryAdministrator

說明：SSO 目錄的管理員存取權

AWSSSODirectoryAdministrator是AWS 受管理的策略。

使用此政策

您可以附加AWSSSODirectoryAdministrator至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 31 日, 世界標準時間 23:54
- 編輯時間：2022 年 10 月 20 日，世界標準時間 20:34
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSSODirectoryReadOnly

說明： ReadOnly SSO 目錄的存取

AWSSSODirectoryReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSSSODirectoryReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 10 月 31 日, 23:49 世界標準時間
- 編輯時間：世界標準時間：二零二二年十一月十六日
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSSOMasterAccountAdministrator

說明：提供 AWS SSO 內的存取權， AWS 以管理 Organizations 主帳戶和成員帳戶以及雲端應用程式

`AWSSSOMasterAccountAdministrator`是AWS 受管理的策略。

使用此政策

您可以附加`AWSSSOMasterAccountAdministrator`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 27 日, 世界標準時間 20:36
- 編輯時間：世界標準時間：2024 年 4 月 26 日凌時 38 分
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSSOMemberAccountAdministrator

說明：提供 AWS SSO 內的存取權， AWS 以管理 Organizations 成員帳戶和雲端應用程式

AWSSSOMemberAccountAdministrator是AWS 受管理的策略。

使用此政策

您可以附加AWSSSOMemberAccountAdministrator至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 27 日, 世界標準時間 20:45
- 編輯時間：2024 年 4 月 26 日，00:31 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSSOReadOnly

描述：提供 AWS SSO 組態的唯讀存取權。

AWSSSOReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSSSOReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 27 日, 世界標準時間 20:24
- 編輯時間：世界標準時間：2024 年 4 月 26 日凌時 44 分
- ARN: arn:aws:iam::aws:policy/AWSSSOReadOnly

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSSOServiceRolePolicy

說明：授予 AWS SSO 許可以代表您管理 AWS 資源，包括 IAM 角色、政策和 SAML IdP。

AWSSSOServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：二零一七年十二月五日 18:36 世界標準時間

- 編輯時間：2022 年 10 月 20 日，世界標準時間 20:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy

政策版本

策略版本：v17(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSStepFunctionsConsoleFullAccess

說明：提供使用者/角色等存取主控台的存取原則。 AWS StepFunctions 為了獲得完整的主控台體驗，除了此政策之外，使用者可能還需要其他 IAM 角色的 iam: PassRole 權限，這些角色可以由服務承擔。

AWSStepFunctionsConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSStepFunctionsConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 11 日, 世界標準時間 21:54
- 編輯時間：2017 年 1 月 12 日，世界標準時間 00:19
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSStepFunctionsFullAccess

說明：提供 API 使用者/角色等存取權限的存取政策。 AWS StepFunctions 若要取得完整存取權，除了此政策之外，使用者還必須擁有至少一個 IAM 角色的 iam: PassRole 權限，該角色可由服務承擔。

AWSStepFunctionsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSStepFunctionsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 11 日, 世界標準時間 21:51
- 編輯時間：2017 年 1 月 11 日，世界標準時間 21:51
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSStepFunctionsReadOnlyAccess

說明：提供使用者/角色/等服務的唯讀存取權限的存取政策。 AWS StepFunctions

AWSStepFunctionsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSStepFunctionsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2017 年 1 月 11 日, 世界標準時間 21:46
- 編輯時間:2024 年 4 月 26 日, 世界標準時間 18:53
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSStorageGatewayFullAccess

說明：透過提供 S AWS torage Gateway 的完整存取 AWS Management Console。

AWSStorageGatewayFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSStorageGatewayFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2022 年 9 月 6 日，世界標準時間 20:26
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSStorageGatewayReadOnlyAccess

說明：提供 AWS 存取 Storage Gateway，透過 AWS Management Console.

`AWSStorageGatewayReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSStorageGatewayReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2022 年 9 月 6 日，世界標準時間 20:24

- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSStorageGatewayServiceRolePolicy

說明：Storage Gateway 用來與 S AWS torage Gateway 整合其他 AWS 服務的服務連結角色。

`AWSStorageGatewayServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2021 年 2 月 17 日，世界標準時間 19:03
- 編輯時間：2021 年 2 月 17 日，世界標準時間 19:03
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSupplyChainFederationAdminAccess

摘要： AWSSupplyChainFederationAdminAccess 提供 AWS 供應鏈同盟使用者存取「 AWS 供應鏈」應用模組，包括在「供應鏈」 AWS 應用模組中執行作業的必要權限。該政策提供 IAM 身分中心使用者和群組的管理許可，並附加至 AWS 供應鏈代表您建立的角色。您不應將 AWSSupplyChainFederationAdminAccess 政策附加到任何其他 IAM 實體。

`AWSSupplyChainFederationAdminAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSSupplyChainFederationAdminAccess`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 2023 年 3 月 1 日, 18:54
- 編輯時間:2023 年 11 月 1 日, 世界標準時間 18:50
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSupportAccess

描述：允許使用者存取「中 AWS Support 心」。

AWSSupportAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSupportAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: arn:aws:iam::aws:policy/AWSSupportAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSupportAppFullAccess

說明：提供對 AWS Support 應用程序和其他必需服務的完整訪問權限，例如 AWS Support 和 Service Quotas。此原則包含使用支援服務的權限，以便使用者可以聯絡 AWS Support 以取得支援案例、變更服務配額，以及建立相關的服務連結角色。

AWSSupportAppFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSupportAppFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 22 日，世界標準時間 16:53
- 編輯時間：2022 年 8 月 22 日，世界標準時間 16:53
- ARN: arn:aws:iam::aws:policy/AWSSupportAppFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSupportAppReadOnlyAccess

說明：提供 AWS Support 應用程式的唯讀存取權。

AWSSupportAppReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSupportAppReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 22 日，世界標準時間 17:01
- 編輯時間：2022 年 8 月 22 日，世界標準時間 17:01
- ARN: arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSupportPlansFullAccess

描述：提供支援計劃的完整存取權。

AWSSupportPlansFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSupportPlansFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：2022 年 9 月 27 日，18:19
- 編輯時間：世界標準時間 2023 年 5 月 9 日晚上 7 時 7 分
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSupportPlansReadOnlyAccess

說明：提供支援計劃的唯讀存取權。

AWSSupportPlansReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSupportPlansReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 9 月 27 日，世界標準時間 18:08
- 編輯時間：世界標準時間：2022 年 9 月 27 日，下午 18 時
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSupportServiceRolePolicy

描述： AWS Support 允許訪問 AWS 資源以提供計費，管理和支持服務。

AWSSupportServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 4 月 19 日, 世界標準時間 18:04
- 編輯時間:2024 年 5 月 2 日, 02:47 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy

政策版本

策略版本：v36(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEventCategories",
        "dms:describeEvents",
        "dms:describeEventSubscriptions",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstances",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "docdb-elastic:getCluster",
        "docdb-elastic:getClusterSnapshot",
        "docdb-elastic:listClusters",
        "docdb-elastic:listClusterSnapshots",
        "drs:describeJobLogItems",
        "drs:describeJobs",
        "drs:describeLaunchConfigurationTemplates",
        "drs:describeRecoveryInstances",
        "drs:describeRecoverySnapshots",
        "drs:describeReplicationConfigurationTemplates",
        "drs:describeSourceNetworks",
        "drs:describeSourceServers",
        "drs:getLaunchConfiguration",
```

```
        "drs:getReplicationConfiguration",
        "drs:listExtensibleSourceServers",
        "drs:listLaunchActions",
        "drs:listStagingAccounts",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTimeToLive",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
```

```
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInternetGateways",
```

```
        "ec2:describeIpamPools",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
```

```
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
```

```
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImages",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImageScanFindings",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:listImages",
        "ecr:listTagsForResource",
```

```
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
```

```
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
```

```
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
        "elastictranscoder:readPreset",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
```

```
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
        "evidently:listSegments",
```

```
        "evidently:listSegmentReferences",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listArchives",
        "events:listApiDestinations",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fms:getAdminAccount",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:listComplianceStatus",
        "fms:listMemberAccounts",
        "fms:listPolicies",
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
```

```
        "forecast:listForecasts",
        "forecast:listPredictors",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "glacier:describeJob",
```

```
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
```

```
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
```

```
        "glue:querySchemaVersionMetadata",
        "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:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
```

```
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
```

```
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEvents",
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
```

```
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
```

```
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
```

```
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
```

```
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
```

```
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express: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"
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSystemsManagerAccountDiscoveryServicePolicy

說明：授予 AWS Systems Manager (SSM) 探索 AWS 帳戶 資訊的權限。

`AWSSystemsManagerAccountDiscoveryServicePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十月二十四日, 世界標準時間
- 編輯時間：2022 年 10 月 17 日，世界標準時間 20:25
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSystemsManagerChangeManagementServicePolicy

描述：可讓您存取「 AWS 系統管理員」變更管理架構所管理或使用的 AWS 資源。

AWSSystemsManagerChangeManagementServicePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 12 月 7 日, 世界標準時間 22:21
- 編輯時間:2020 年十二月 7 日, 世界標準時間 22:21

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSystemsManagerForSAPFullAccess

描述：提供 SAP 服務 AWS Systems Manager 的完整存取權

AWSSystemsManagerForSAPFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSystemsManagerForSAPFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間十一月十七日，下午 2:11
- 編輯時間：2022 年十一月十八日，世界標準時間 21:58
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSystemsManagerForSAPReadOnlyAccess

描述：提供 SAP 服務之 AWS Systems Manager 的唯讀存取權

AWSSystemsManagerForSAPReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSSystemsManagerForSAPReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間十一月十七日，下午 2:11
- 編輯時間：世界標準時間十一月十七日，二○二二年
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSSystemsManagerOpsDataSyncServiceRolePolicy

說明：SSM 總管用來管理 OpsData 相關作業的 IAM 角色

AWSSystemsManagerOpsDataSyncServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 4 月 26 日, 世界標準時間 20:42
- 編輯時間:2023 年 6 月 28 日, 世界標準時間 22:53
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSThinkboxAssetServerPolicy

描述：此原則會授與入 AWS 口網站資產伺服器正常作業所需的必要權限。

AWSThinkboxAssetServerPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSThinkboxAssetServerPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 27 日, 世界標準時間 19:18
- 編輯時間:2020 年 5 月 27 日, 世界標準時間 19:18
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSThinkboxAWSPortalAdminPolicy

描述：此政策授予 AWS Thinkbox 的截止日期軟體完全存取入 AWS 口網站管理所需的多項 AWS 服務。這包括在多個 EC2 資源類型上建立任意標籤的存取權。

AWSThinkboxAWSPortalAdminPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSThinkboxAWSPortalAdminPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 27 日, 世界標準時間 19:41
- 編輯時間:世界標準時間 2024 年 4 月 12 日, 20:07
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSThinkboxAWSPortalGatewayPolicy

說明：此原則會授與入 AWS 口網站閘道機器正常作業所需的必要權限。

AWSThinkboxAWSPortalGatewayPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSThinkboxAWSPortalGatewayPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 27 日, 世界標準時間 19:05
- 編輯時間：2020 年 6 月 30 日，世界標準時間 16:02
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "dynamodb:Scan",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSThinkboxAWSPortalWorkerPolicy

描述：此原則會授與 AWS 入口網站中的「截止日期工作者」正常作業所需的必要權限。

AWSThinkboxAWSPortalWorkerPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSThinkboxAWSPortalWorkerPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 27 日, 世界標準時間 19:15
- 編輯時間:2020 年十二月 7 日, 世界標準時間 23:27
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSThinkboxDeadlineResourceTrackerAccessPolicy

描述：授予 AWS Thinkbox 的截止日期資源跟踪器操作所需的權限。這包括對某些 EC2 動作的完整存取權，包括 DeleteFleets 和 CancelSpotFleetRequests。

AWSThinkboxDeadlineResourceTrackerAccessPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSThinkboxDeadlineResourceTrackerAccessPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 27 日, 世界標準時間 19:25
- 編輯時間:2020 年 5 月 27 日, 世界標準時間 19:25
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
      ]
    }
```

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSThinkboxDeadlineResourceTrackerAdminPolicy

描述：授予創建，銷毀和管理 AWS Thinkbox 的截止日期資源跟踪器所需的權限。

AWSThinkboxDeadlineResourceTrackerAdminPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSThinkboxDeadlineResourceTrackerAdminPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 27 日, 世界標準時間 19:29
- 編輯時間：世界標準時間 2024 年 4 月 12 日，20:55
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

描述：授予 AWS Thinkbox 的截止日期現貨事件插件所需的權限。這包括請求、修改和取消競價型叢集的權限，以及有限的 PassRole 權限。

AWSThinkboxDeadlineSpotEventPluginAdminPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSThinkboxDeadlineSpotEventPluginAdminPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 27 日, 世界標準時間 19:38
- 編輯時間：2020 年 5 月 27 日，世界標準時間 19:38
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

說明：授予執行 AWS Thinkbox 期限 Spot 事件外掛程式工作者軟體的 EC2 執行個體所需的許可。

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy是AWS 受管理的策略。

使用此政策

您可以附加AWSThinkboxDeadlineSpotEventPluginWorkerPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 27 日, 世界標準時間 19:35
- 編輯時間：2020 年 12 月 7 日，世界標準時間 23:31

- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSTransferConsoleFullAccess

說明：提供 AWS 傳輸的完整存取權 AWS Management Console

AWSTransferConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSTransferConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十四日, 世界標準時間 19:33
- 編輯時間：2020 年十二月十四日，世界標準時間 19:33
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSTransferFullAccess

描述：提供 AWS 轉移服務的完整存取權。

AWSTransferFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSTransferFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十四日, 世界標準時間 19:37
- 編輯時間：2020 年十二月十四日，世界標準時間 19:37
- ARN: arn:aws:iam::aws:policy/AWSTransferFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSTransferLoggingAccess

說明：允許 AWS 傳送完整存取權以建立記錄串流和群組，並將記錄事件放入您的帳戶

AWSTransferLoggingAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSTransferLoggingAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2019 年 1 月 14 日, 世界標準時間 15:32
- 編輯時間：2019 年 1 月 14 日，世界標準時間 15:32
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
```

```
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSTransferReadOnlyAccess

描述：提供 AWS 轉移服務的唯讀存取權。

AWSTransferReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSTransferReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 27 日, 世界標準時間 17:54
- 編輯時間:2020 年 8 月 27 日, 世界標準時間 17:54
- ARN: arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSTrustedAdvisorPriorityFullAccess

說明：提供「 AWS Trusted Advisor 優先順序」的完整 此原則也可讓使用者將 AWS Trusted Advisor 新增為 Organizations 的信任服務，並指定「受 Trusted Advisor 優先順序」的委派管理員帳戶。

`AWSTrustedAdvisorPriorityFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSTrustedAdvisorPriorityFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 16 日，世界標準時間 16:08
- 編輯時間：2022 年 8 月 16 日，世界標準時間 16:08
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
```

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSTrustedAdvisorPriorityReadOnlyAccess

說明：提供 AWS Trusted Advisor 優先順序的唯讀存取權 這包括檢視委派管理員帳戶的權限。

`AWSTrustedAdvisorPriorityReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSTrustedAdvisorPriorityReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 16 日，世界標準時間 16:35
- 編輯時間：2022 年 8 月 16 日，世界標準時間 16:35
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSTrustedAdvisorReportingServiceRolePolicy

說明：受 Trusted Advisor 多帳戶報告的服務政策

AWSTrustedAdvisorReportingServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月十九日, 世界時間 17:41
- 編輯時間：世界標準時間 2023 年 2 月 28 日 23:23
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSTrustedAdvisorServiceRolePolicy

描述：存取 AWS 受信任的顧問服務，以協助降低成本、提高效能，以及改善 AWS 環境的安全性。

AWSTrustedAdvisorServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 2 月 22 日, 世界標準時間 21:24
- 編輯時間:2024 年 1 月 18 日, 世界標準時間 16:25
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy

政策版本

策略版本：v12(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpnConnections",
```

```
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "kinesis:DescribeLimits",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
```

```
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSUserNotificationsServiceLinkedRolePolicy

描述：允許「 AWS 使用者通知」代表您撥打 AWS 服務。

`AWSUserNotificationsServiceLinkedRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2023 年 4 月 19 日, 13:28
- 編輯時間：世界標準時間 2023 年 4 月 19 日 , 13:28
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSVendorInsightsAssessorFullAccess

描述：提供完整存取權以檢視有權供應商見解資源和管理廠商洞察訂閱

AWSVendorInsightsAssessorFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSVendorInsightsAssessorFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 7 月 26 日, 下午 3:05
- 編輯時間：世界標準時間：2022 年十二月一日凌晨 51 分
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
```

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSVendorInsightsAssessorReadOnly

描述：提供唯讀存取權以檢視有權供應商見解資源

AWSVendorInsightsAssessorReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSVendorInsightsAssessorReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 7 月 26 日, 下午 3:05
- 編輯時間：世界標準時間（世界標準時間）12 月 1 日
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSVendorInsightsVendorFullAccess

描述：提供創建和管理供應商洞察資源的完整訪問權限

AWSVendorInsightsVendorFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSVendorInsightsVendorFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 7 月 26 日, 下午 3:05
- 編輯時間：世界標準時間：2023 年 10 月 19 日凌晨 1 時 41 分
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSVendorInsightsVendorReadOnly

描述：提供唯讀存取權以檢視供應商洞察資源

AWSVendorInsightsVendorReadOnly是AWS 受管理的策略。

使用此政策

您可以附加AWSVendorInsightsVendorReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 7 月 26 日, 下午 3:05
- 編輯時間：世界標準時間（世界標準時間）12 月 1 日
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSVpcLatticeServiceRolePolicy

說明：允許 VPC 格代表您存取 AWS 資源。

AWSVpcLatticeServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：二○二二年十一月三十日，世界標準時間
- 編輯時間：2022 年十一月三十日，世界標準時間 20:47
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSVPCS2SVpnServiceRolePolicy

說明：允許 Site-to-Site VPN 建立和管理與 VPN 連線相關的資源。

AWSVPCS2SVpnServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 8 月 6 日, 14:13 世界標準時間
- 編輯時間：2019 年 8 月 6 日，世界標準時間 14:13
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSVPCTransitGatewayServiceRolePolicy

說明：允許 VPC Transit Gateway 為傳 Transit Gateway 道 VPC 附件建立和管理必要的資源。

`AWSVPCTransitGatewayServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月二十六日, 世界標準時間 16:21
- 編輯時間：2021 年 4 月 15 日，世界標準時間 16:31
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AssignIpv6Addresses",
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Sid" : "0"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSVPCVerifiedAccessServiceRolePolicy

說明：啟用「 AWS 已驗證存取」服務以代表您佈建端點的政策

AWSVPCVerifiedAccessServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間十一月二十九日，下午 3:35
- 編輯時間：世界標準時間 2023 年 11 月 17 日晚上 9 點 3 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSWAFConsoleFullAccess

說明：透過提供 AWS WAF 的 AWS Management Console完整存取權。請注意，此政策還授予列出和更新 Amazon CloudFront 分發的許可、在 E AWS lastic Load Balancing 上檢視負載平衡器的許可、檢視 Amazon API Gateway REST API 和階段的許可、列出和檢視 Amazon CloudWatch 指標的許可，以及檢視帳戶內已啟用區域的許可。

AWSWAFConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSWAFConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 6 日, 世界標準時間 18:38
- 編輯時間：2023 年 6 月 5 日，世界標準時間 20:56
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSWAFConsoleReadOnlyAccess

描述：透過提供 AWS WAF 的 AWS Management Console唯讀存取權。請注意，此政策還授予列出 Amazon CloudFront 分發的許可、在 E AWS lastic Load Balancing 上檢視負載平衡器的許可、檢視 Amazon API Gateway REST API 和階段的許可、列出和檢視 Amazon CloudWatch 指標的許可，以及檢視帳戶內已啟用區域的許可。

AWSWAFConsoleReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSWAFConsoleReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 6 日, 世界標準時間 18:43
- 編輯時間：2023 年 6 月 5 日，世界標準時間 20:56
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSWAFFullAccess

描述：提供 AWS WAF 動作的完整存取權。

AWSWAFFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSWAFFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 10 月 6 日, 世界標準時間 20:44
- 編輯時間:2023 年 6 月 5 日, 世界標準時間 20:55
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSWAFReadOnlyAccess

描述：提供 AWS WAF 動作的唯讀存取權。

AWSWAFReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSWAFReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 10 月 6 日, 世界標準時間 20:43
- 編輯時間:2023 年 6 月 5 日, 世界標準時間 20:55
- ARN: arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSWellArchitectedDiscoveryServiceRolePolicy

描述： WellArchitected 允許代表客戶存取與資 WellArchitected 源相關的 AWS 服務和資源。

AWSWellArchitectedDiscoveryServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 4 月 26 日, 世界標準時間 18:36
- 編輯時間:世界標準時間 2023 年 4 月 26 日, 18:36
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:GetApplication",
        "servicecatalog:CreateAttributeGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/applications/*",
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSWellArchitectedOrganizationsServiceRolePolicy

描述：允許 Well-Architected 代表您存取 Organizations。

`AWSWellArchitectedOrganizationsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：2022 年 6 月 23 日，17:15
- 編輯時間：世界標準時間：2022 年 7 月 25 日，下午 18:03
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSWickrFullAccess

描述：此原則會授與 Wickr 服務的完整管理權限，包括. AWS Management Console

`AWSWickrFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSWickrFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：二零二二年十一月二十七
- 編輯時間：2022 年十一月二十七日，世界標準時間 20:36
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSXrayCrossAccountSharingConfiguration

描述：提供管理可觀測性存取管理員連結和建立 X-Ray 軌跡共用的功能

AWSXrayCrossAccountSharingConfiguration是AWS 受管理的策略。

使用此政策

您可以附加AWSXrayCrossAccountSharingConfiguration至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：二零二年十一月二十七日

- 編輯時間：2022 年十一月二十七日，世界標準時間下午
- ARN: arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
      ]
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSXRayDaemonWriteAccess

描述：允許 AWS X-Ray 精靈將原始追蹤區段資料轉送至服務的 API，並擷取 X-Ray SDK 要使用的取樣資料 (規則、目標等)。

AWSXRayDaemonWriteAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSXRayDaemonWriteAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 8 月 28 日, 世界標準時間下午 11 點
- 編輯時間：世界標準時間 2024 年 2 月 13 日晚上 9 時 58 分
- ARN: arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSXrayFullAccess

說明： AWS X-Ray 完全存取管理原則

AWSXrayFullAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSXrayFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2016 年 12 月 1 日下午 6 時 30 分
- 編輯時間：世界標準時間 2024 年 4 月 11 日下午 17 時 7 分
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSXrayReadOnlyAccess

說明： AWS X-Ray 唯讀受管政策

AWSXrayReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加AWSXrayReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年十二月 1 日, 18:27 世界標準時
- 編輯時間：2024 年 2 月 14 日，00:35 世界標準時間
- ARN: arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSXrayWriteOnlyAccess

描述： AWS X-Ray 僅寫入受管理的原則

`AWSXrayWriteOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`AWSXrayWriteOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**二零一六年十二月 1 日, 18:19 世界標準時
- **編輯時間:**2018 年 8 月 28 日, 世界標準時間 23:03
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

AWSZonalAutoshiftPracticeRunSLRPolicy

描述：提供 ARC 區域輪班練習運行的管理訪問權限，並提供 CloudWatch 警報狀態以監控練習運行的訪問權限。

AWSZonalAutoshiftPracticeRunSLRPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 29 日下午 17 時 34 分
- 編輯時間：世界標準時間 2023 年 11 月 29 日下午 17 時 34 分
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

BatchServiceRolePolicy

說明：提供 AWS Batch 服務的存取權，以管理所需的資源，包括 Amazon EC2 和 Amazon ECS 資源。

`BatchServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 3 月 10 日, 06:55 世界標準時間
- 編輯時間：世界標準時間 2023 年 12 月 5 日晚上 22 時 52 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

Billing

描述：授予帳單和成本管理的權限。這包括檢視帳戶使用情況，以及檢視與修改預算與付款方式。

Billing是AWS 受管理的策略。

使用此政策

您可以附加Billing至您的使用者、群組和角色。

政策詳情

- 類型：Job 職能政策
- 創建時間:二零一六年十一月十日, 17:33 世界標準時
- 編輯時間：世界標準時間 2024 年 1 月 17 日下午 18:03
- ARN: arn:aws:iam::aws:policy/job-function/Billing

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:UpdateBillingPreferences",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
```

```
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:TagResource",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
        "ce:UntagResource",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
```

```
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CertificateManagerServiceRolePolicy

說明：Amazon Certificate Manager 服務角色政策

`CertificateManagerServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 6 月 25 日, 世界標準時間 17:56
- 編輯時間:2020 年 6 月 25 日, 世界標準時間 17:56
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ClientVPNServiceConnectionsRolePolicy

說明：啟用 AWS Client VPN 管理 Client VPN 端點連線的原則。

`ClientVPNServiceConnectionsRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 8 月 12 日, 世界標準時間 19:48
- 編輯時間：2020 年 8 月 12 日，世界標準時間 19:48
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
```

```
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ClientVPNServiceRolePolicy

說明：啟用 AWS Client VPN 管理 Client VPN 端點的政策。

`ClientVPNServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一八年十二月十日 21:20 世界標準時間
- 編輯時間:2020 年 8 月 12 日, 世界標準時間 19:39
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudFormationStackSetsOrgAdminServiceRolePolicy

摘要： CloudFormation StackSets (組織主要帳戶) 的服務角色

`CloudFormationStackSetsOrgAdminServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：二零一九年十二月十日 00:20 世界標準時間
- 編輯時間：2019 年 12 月 10 日，世界標準時間 00:20
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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-*"
    }
```

```
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudFormationStackSetsOrgMemberServiceRolePolicy

摘要： CloudFormation StackSets (組織成員帳戶) 的服務角色

`CloudFormationStackSetsOrgMemberServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：二零一九年十二月九日 23:52 世界標準時間
- 編輯時間：二零一九年十二月九日 23:52 世界標準時間
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudFrontFullAccess

說明：提供對 CloudFront 主控台的完整存取權，Amazon S3 及透過 AWS Management Console.

`CloudFrontFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加CloudFrontFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間:2024 年 1 月 4 日, 世界標準時間 16:56
- ARN: arn:aws:iam::aws:policy/CloudFrontFullAccess

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
```

```
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "cffdescribestream",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudFrontReadOnlyAccess

描述：可透過 AWS Management Console. CloudFront

`CloudFrontReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加CloudFrontReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間:2024 年 1 月 4 日, 世界標準時間 16:55
- ARN: arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudHSMServiceRolePolicy

描述：可存取 CloudHSM 所使用或管理的 AWS 資源

CloudHSMServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年 11 月 6 日，世界標準時間 19:12
- 編輯時間：2017 年 11 月 6 日，世界標準時間 19:12
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudSearchFullAccess

描述：提供對 Amazon CloudSearch 組態服務的完整存取權。

`CloudSearchFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudSearchFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間

- 編輯時間:2015 年 2 月 6 日, 18:39 世界標準時間
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudSearchReadOnlyAccess

說明：提供 Amazon CloudSearch 組態服務的唯讀存取權。

`CloudSearchReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加CloudSearchReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間:2015 年 2 月 6 日, 18:39 世界標準時間
- ARN: arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudTrailServiceRolePolicy

描述：權限政策 CloudTrail ServiceLinkedRole

CloudTrailServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 10 月 24 日, 21:21 世界標準時間
- 編輯時間:2023 年 11 月 27 日, 01:18 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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}"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatch-CrossAccountAccess

說明： CloudWatch 允許假設 CloudWatch-代表當前帳戶的遠程帳戶中的CrossAccountSharing 角色，以便跨帳戶，跨區域顯示數據

`CloudWatch-CrossAccountAccess`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 7 月 23 日, 09:59 世界標準時間
- 編輯時間:2019 年 7 月 23 日, 09:59 世界標準時間
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchActionsEC2Access

說明：提供 CloudWatch 警示和指標以及 EC2 中繼資料的唯讀存取權。提供對停止、終止和重新啟動 EC2 執行個體的存取權。

`CloudWatchActionsEC2Access`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchActionsEC2Access`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- 創建時間:2015 年 7 月 7 日, 00:00 世界標準時間
- 編輯時間:2015 年 7 月 7 日, 00 世界標準時間
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchAgentAdminPolicy

描述：使用所需的完整權限 AmazonCloudWatchAgent。

CloudWatchAgentAdminPolicy是AWS 受管理的策略。

使用此政策

您可以附加CloudWatchAgentAdminPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 7 日, 00:52 世界標準時間
- 編輯時間：世界標準時間 2024 年 2 月 5 日，20:59
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchAgentServerPolicy

說明： AmazonCloudWatchAgent 在伺服器上使用所需的權限

`CloudWatchAgentServerPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchAgentServerPolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 3 月 7 日, 世界標準時間 01:06
- 編輯時間：世界標準時間 2024 年 2 月 6 日，16:37
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchApplicationInsightsFullAccess

描述：提供對 CloudWatch 應用程式深入解析和必要相依性的完整存取

`CloudWatchApplicationInsightsFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchApplicationInsightsFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十一月二十四日, 世界標準時間 18:44
- 編輯時間：2022 年 1 月 25 日，世界標準時間 17:51
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchApplicationInsightsReadOnlyAccess

描述：提供「CloudWatch 應用程式見解」的唯讀存取權。

`CloudWatchApplicationInsightsReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchApplicationInsightsReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十一月二十四日, 世界標準時間 18:48

- 編輯時間:2020 年十一月二十四日, 世界標準時間 18:48
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudwatchApplicationInsightsServiceLinkedRolePolicy

說明：Cloudwatch 應用程式洞察服務連結的角色政策

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2018 年 12 月 1 日, 16:22
- 編輯時間：2023 年 5 月 11 日，世界標準時間 16:34
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

政策版本

策略版本：v24(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
```

```
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchApplicationSignalsServiceRolePolicy

說明：政策授予「CloudWatch 應用程式訊號」的權限，以便從其他相關 AWS 服務收集監控和標記資料。

`CloudWatchApplicationSignalsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 11 月 9 日，18:09
- 編輯時間：世界標準時間 2024 年 4 月 26 日晚上 9 時 29 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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}"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchAutomaticDashboardsAccess

描述：提供存取用於顯示 CloudWatch 自動儀表板的非 CloudWatch API，包括物件的內容，例如 Lambda 函數

`CloudWatchAutomaticDashboardsAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchAutomaticDashboardsAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 7 月 23 日, 世界標準時間 10:01
- 編輯時間:2021 年 4 月 20 日, 世界標準時間 13:05
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchCrossAccountSharingConfiguration

描述：提供管理可觀察性存取管理員連結和建立資源共用的 CloudWatch 功能

`CloudWatchCrossAccountSharingConfiguration`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchCrossAccountSharingConfiguration`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間十一月二十七日，下午四時
- 編輯時間：二零二二年十一月二十七日，世界標準時
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchEventsBuiltInTargetExecutionAccess

說明：允許 Amazon CloudWatch 事件中的內建目標代表您執行 EC2 動作。

`CloudWatchEventsBuiltInTargetExecutionAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchEventsBuiltInTargetExecutionAccess`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：二零一六年一月十四日 18:35 世界標準時間
- 編輯時間:2016 年 1 月 14 日, 世界標準時間 18:35
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchEventsFullAccess

描述：提供對 Amazon CloudWatch 活動的完整訪問權限。

CloudWatchEventsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加CloudWatchEventsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2016 年 1 月 14 日, 世界標準時間 18:37
- 編輯時間：世界標準時間：2022 年 12 月 1 日，下午 5 時
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchEventsInvocationAccess

說明：允許 Amazon CloudWatch 事件將事件轉送到您帳戶中 AWS Kinesis 串流中的串流。

`CloudWatchEventsInvocationAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchEventsInvocationAccess`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：二零一六年一月十四日 18:36 世界標準時間
- 編輯時間:2016 年 1 月 14 日, 世界標準時間 18:36
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchEventsReadOnlyAccess

描述：提供 Amazon CloudWatch 活動的唯讀存取權。

CloudWatchEventsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加CloudWatchEventsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2016 年 1 月 14 日, 世界標準時間 18:27

- **編輯時間：世界標準時間：2022 年 12 月 1 日，下午 16 點**
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchEventsServiceRolePolicy

描述： AWS CloudWatch 允許代表您執行通過警報和事件配置的操作。

`CloudWatchEventsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年十一月十七日，世界標準時間 00:42
- 編輯時間：2017 年十一月十七日，世界標準時間 00:42
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchFullAccess

描述：提供對的完整存取權 CloudWatch。

`CloudWatchFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2022 年十一月二十七日，世界標準時間下午
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchFullAccessV2

描述：提供對的完整存取權 CloudWatch。

CloudWatchFullAccessV2是AWS 受管理的策略。

使用此政策

您可以附加CloudWatchFullAccessV2至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2023 年 8 月 1 日, 上午 11:32 世界標準時間
- 編輯時間：世界標準時間 2023 年 12 月 5 日，下午 19:36
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
```

```
        "iam:GetRole",
        "oam:ListSinks",
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchInternetMonitorServiceRolePolicy

說明：允許網際網路監控器代表您存取 EC2、工作區和 CloudFront 資源，以及其他必要的服務。

`CloudWatchInternetMonitorServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：二零二年十一月二十七日
- 編輯時間：世界標準時間 7 月 20 日，2023 年 4 月 46 日
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchLambdaInsightsExecutionRolePolicy

說明：Lambda 見解延伸模組所需的政策

CloudWatchLambdaInsightsExecutionRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加CloudWatchLambdaInsightsExecutionRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 10 月 7 日, 世界標準時間 19:27
- 編輯時間:2020 年 10 月 7 日, 世界標準時間 19:27
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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:*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchLogsCrossAccountSharingConfiguration

描述：提供管理可觀測性存取管理員連結和建立 CloudWatch 記錄資源共用的功能

`CloudWatchLogsCrossAccountSharingConfiguration`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchLogsCrossAccountSharingConfiguration`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二 ○ 二 ○ 二年十一月二十七日，下午三時
- 編輯時間：2022 年十一月二十七日，世界標準時間 13:55
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchLogsFullAccess

描述：提供 CloudWatch 記錄檔的完整存取權

`CloudWatchLogsFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchLogsFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間:2023 年 11 月 26 日, 世界標準時間 18:12
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchLogsReadOnlyAccess

說明：提供 CloudWatch 記錄檔的唯讀存取權

`CloudWatchLogsReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchLogsReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2023 年 11 月 26 日晚上 18 時 11 分
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchNetworkMonitorServiceRolePolicy

描述：允許 CloudWatch 網路監控器代表您存取和管理 EC2 和 VPC 資源、將資料發佈到以 CloudWatch 及存取其他必要的服務。

CloudWatchNetworkMonitorServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 12 月 21 日，18:53
- 編輯時間：世界標準時間 2023 年 12 月 21 日下午 18:53
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchReadOnlyAccess

描述：提供的唯讀存取權 CloudWatch。

CloudWatchReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加CloudWatchReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：世界標準時間 2023 年 12 月 5 日，下午 19:24
- ARN: arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchSyntheticsFullAccess

描述：提供對 CloudWatch Synthetics 的完全訪問權限。

CloudWatchSyntheticsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加CloudWatchSyntheticsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月二十五日, 下午 17 點 39
- 編輯時間：2022 年 5 月 6 日，世界標準時間 18:14
- ARN: arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess

政策版本

策略版本：v9(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CloudWatchSyntheticsReadOnlyAccess

描述：提供 CloudWatch Synthetics 的唯讀訪問權限。

`CloudWatchSyntheticsReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`CloudWatchSyntheticsReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十一月二十五日, 世界標準時
- 編輯時間：2020 年 3 月 6 日，世界標準時間 19:26
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ComprehendDataAccessRolePolicy

說明：允許存取 S3 資源以進行資料存取的 AWS Comprehend 服務角色的政策

`ComprehendDataAccessRolePolicy`是AWS 受管理的策略。

使用此政策

您可以附加`ComprehendDataAccessRolePolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：二零一九年三月六日, 世界標準時間 22:28

- 編輯時間：2019 年 3 月 6 日，世界標準時間 22:28
- ARN: arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ComprehendFullAccess

描述：提供對 Amazon Comprehend 的完整存取權。

ComprehendFullAccess是AWS 受管理的策略。

使用此政策

您可以附加ComprehendFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月二十九日，世界標準時間 18:08
- 編輯時間:十二月五日, 2017, 01:36 世界標準時間
- ARN: arn:aws:iam::aws:policy/ComprehendFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ComprehendMedicalFullAccess

描述：提供對亞馬遜綜合醫療的完整訪問

ComprehendMedicalFullAccess是AWS 受管理的策略。

使用此政策

您可以附加ComprehendMedicalFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十七日, 世界標準時間 17:55
- 編輯時間:2018 年十一月二十七日, 世界標準時間 17:55
- ARN: arn:aws:iam::aws:policy/ComprehendMedicalFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ComprehendReadOnly

描述：提供對 Amazon Comprehend 的唯讀存取權。

`ComprehendReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`ComprehendReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月二十九日，世界標準時間 18:10
- 編輯時間：2022 年 4 月 26 日，世界標準時間 21:32
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ComputeOptimizerReadOnlyAccess

描述：提供的唯讀存取權 ComputeOptimizer。

`ComputeOptimizerReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`ComputeOptimizerReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 3 月 7 日，世界標準時間 00:11
- 編輯時間:2023 年 8 月 28 日, 世界標準時間 19:22
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
```

```
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ComputeOptimizerServiceRolePolicy

描述：允許 ComputeOptimizer 代表您呼叫 AWS 服務並收集工作負載詳細資料。

`ComputeOptimizerServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十二月三日, 08:45 世界標準時
- 編輯時間：2022 年 6 月 13 日，世界標準時間 19:05
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ConfigConformsServiceRolePolicy

描述：建立一致性套 AWSConfig 件所需的原則

`ConfigConformsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 7 月 25 日, 世界標準時間 21:38
- 編輯時間:2023 年 1 月 12 日, 04:17 世界標準時間
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CostOptimizationHubAdminAccess

描述：此受管理原則可讓管理員存取成本最佳化中樞。

CostOptimizationHubAdminAccess是AWS 受管理的策略。

使用此政策

您可以附加CostOptimizationHubAdminAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 12 月 19 日，00:03
- 編輯時間：世界標準時間 2023 年 12 月 19 日凌時 03 分
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CostOptimizationHubReadOnlyAccess

描述：此受管理的原則提供成本最佳化中樞的唯讀存取權。

CostOptimizationHubReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加CostOptimizationHubReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 12 月 13 日, 18:04
- 編輯時間：世界標準時間 2023 年 12 月 13 日下午 18:04
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CostOptimizationHubServiceRolePolicy

描述：允許成本最佳化中樞擷取組織資訊，並收集與最佳化相關的資料和中繼資料。

CostOptimizationHubServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2023 年 11 月 26 日, 世界標準時間 8:03
- 編輯時間:2023 年 11 月 26 日, 世界標準時間 8:03
- ARN: arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

CustomerProfilesServiceLinkedRolePolicy

描述：允許 Amazon Connect 客戶設定檔代表您存取 AWS 服務和資源。

CustomerProfilesServiceLinkedRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2023 年 3 月 7 日, 22:56
- 編輯時間:世界標準時間 2023 年 3 月 7 日, 22:56
- ARN: arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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_*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

DatabaseAdministrator

描述：授與設定 AWS 資料庫 AWS 服務所需之服務和動作的完整存取權限。

`DatabaseAdministrator`是AWS 受管理的策略。

使用此政策

您可以附加`DatabaseAdministrator`至您的使用者、群組和角色。

政策詳情

- 類型：Job 職能政策
- 創建時間：二零一六年十一月十日 17:25 世界標準時間
- 編輯時間：2019 年 1 月 8 日，世界標準時間 00:48
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

DataScientist

說明：授予 AWS 資料分析服務的權限。

DataScientist是AWS 受管理的策略。

使用此政策

您可以附加DataScientist至您的使用者、群組和角色。

政策詳情

- 類型：Job 職能政策
- 創建時間:二零一六年十一月十日, 17:28 世界標準時

- 編輯時間：2019 年 12 月 3 日，世界標準時間 16:48
- ARN: arn:aws:iam::aws:policy/job-function/DataScientist

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

DAXServiceRolePolicy

描述：此原則允許 DAX 代表客戶建立和管理網路介面、安全性群組、子網路和 VPC

DAXServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 3 月 5 日, 世界標準時間 17:51
- 編輯時間：2018 年 3 月 5 日，世界標準時間 17:51
- ARN: arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

說明：支援 Amazon Amazon DynamoDB 的亞馬遜 CloudWatch 參與者深入解析所需的許可。

DynamoDBCloudWatchContributorInsightsServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十一月十五日, 21:13 世界時間
- 編輯時間：2019 年 11 月 15 日，世界標準時間 21:13
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

DynamoDBKinesisReplicationServiceRolePolicy

描述：提供 AWS DynamoDB 目的存取權 KinesisDataStreams

DynamoDBKinesisReplicationServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2020 年十一月十二日，世界標準時間 00:43
- 編輯時間：2020 年十一月十二日，世界標準時間 00:43
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

DynamoDBReplicationServiceRolePolicy

說明：DynamoDB 跨區域資料複寫所需的權限

DynamoDBReplicationServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2017 年 11 月 9 日，世界標準時間 23:55
- 編輯時間：世界標準時間 2024 年 1 月 8 日晚上 20:10
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

EC2FastLaunchFullAccess

說明：此政策授予 EC2 快速啟動動作的完整存取權

EC2FastLaunchFullAccess是AWS 受管理的策略。

使用此政策

您可以附加EC2FastLaunchFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2024 年 5 月 13 日, 世界標準時間 22:45
- 編輯時間:2024 年 5 月 13 日, 世界標準時間 22:45
- ARN: arn:aws:iam::aws:policy/EC2FastLaunchFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

EC2FastLaunchServiceRolePolicy

說明：政策授予 ec2fastlaunch，以準備和管理客戶帳戶中預先佈建的快照並發布相關指標。

`EC2FastLaunchServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：二零二二年一月十日，世界標準時間 13:08
- 編輯時間：2022 年 1 月 10 日，世界標準時間 13:08
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

EC2FleetTimeShiftableServiceRolePolicy

說明：政策授予 EC2 叢集許可以在 future 啟動執行個體。

`EC2FleetTimeShiftableServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十二月二十三日, 19:47 世界標
- 編輯時間：2019 年十二月二十三日，世界標準時間 19:47
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

Ec2ImageBuilderCrossAccountDistributionAccess

說明：EC2 Image Builder 需要許可才能執行跨帳戶分發。

`Ec2ImageBuilderCrossAccountDistributionAccess`是AWS 受管理的策略。

使用此政策

您可以附加`Ec2ImageBuilderCrossAccountDistributionAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2020 年 9 月 30 日，世界標準時間 19:22
- 編輯時間：2020 年 9 月 30 日，世界標準時間 19:22
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

EC2ImageBuilderLifecycleExecutionPolicy

說明：EC2 ImageBuilderLifecycleExecutionPolicy 政策授予 Image Builder 執行動作 (例如棄用或刪除 Image Builder 資源及其基礎資源 (AMI、快照) 的許可，以支援映像生命週期管理工作的自動化規則。

EC2ImageBuilderLifecycleExecutionPolicy是AWS 受管理的策略。

使用此政策

您可以附加EC2ImageBuilderLifecycleExecutionPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 2023 年 11 月 16 日 23:23
- 編輯時間：世界標準時間 2023 年 11 月 16 日 23:23
- ARN: arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "DeprecatedBy"
        }
      }
    },
    {
      "Sid" : "ECRImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ImageBuilderEC2TagServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "tag:GetResources",
        "imagebuilder:DeleteImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

EC2InstanceConnect

說明：允許客戶呼叫 EC2 執行個體 Connect，將暫時金鑰發佈到其 EC2 執行個體，並透過 ssh 或 EC2 執行個體連線 CLI 進行連線。

EC2InstanceConnect是AWS 受管理的策略。

使用此政策

您可以附加EC2InstanceConnect至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- 創建時間:2019 年 6 月 27 日, 世界標準時間 18:53
- 編輯時間:2019 年 6 月 27 日, 世界標準時間 18:53
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

Ec2InstanceConnectEndpoint

說明：用於管理客戶建立的 EC2 執行個體 Connect 端點的 EC2 執行個體 Connect 端點

Ec2InstanceConnectEndpoint是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 2023 年 1 月 24 日, 20:19
- 編輯時間：世界標準時間 2023 年 1 月 24 日晚上 20:19
- ARN: arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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-*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

EC2InstanceProfileForImageBuilder

說明：Image Builder 服務的 EC2 執行個體設定檔。

`EC2InstanceProfileForImageBuilder`是AWS 受管理的策略。

使用此政策

您可以附加`EC2InstanceProfileForImageBuilder`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月 1 日, 世界標準時間 19:

- **編輯時間**：2020 年 8 月 27 日，世界標準時間 16:40
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

EC2InstanceProfileForImageBuilderECRContainerBuilds

說明：使用 EC2 Image Builder 建立容器映像的 EC2 執行個體設定檔。此原則授與使用者上傳 ECR 影像的廣泛權限。

EC2InstanceProfileForImageBuilderECRContainerBuilds是AWS 受管理的策略。

使用此政策

您可以附加EC2InstanceProfileForImageBuilderECRContainerBuilds至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十二月十一日, 世界標準時間 19:48

- 編輯時間：2020 年十二月十一日，世界標準時間 19:48
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ECRReplicationServiceRolePolicy

描述：啟用 ECR 複製所使用或管理的資源 AWS 服務 和存取權

ECRReplicationServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 12 月 4 日, 世界標準時間 22:11
- 編輯時間：2020 年 12 月 4 日，世界標準時間 22:11
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElastiCacheServiceRolePolicy

描述：此原則可 ElastiCache 讓您視需要管理快取而代表您管理 AWS 資源

`ElastiCacheServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 12 月 7 日, 世界標準時間 17:50
- 編輯時間：世界標準時間十一月二十八日，下午五時五分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElasticLoadBalancingFullAccess

描述：提供對 Amazon 的完整存取權限 ElasticLoadBalancing，以及對提供 ElasticLoadBalancing 功能所需的其他服務的有限存取權。

`ElasticLoadBalancingFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`ElasticLoadBalancingFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 9 月 20 日, 世界標準時間 20:42
- 編輯時間：2022 年十一月二十九日，世界標準時間 1:45
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElasticLoadBalancingReadOnly

說明：提供對 Amazon ElasticLoadBalancing 和相依服務的唯讀存取

ElasticLoadBalancingReadOnly是AWS 受管理的策略。

使用此政策

您可以附加ElasticLoadBalancingReadOnly至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 9 月 20 日, 世界標準時間 20:17
- 編輯時間:2023 年 11 月 26 日, 世界標準時間 18:15
- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElementalActivationsDownloadSoftwareAccess

說明：檢視購買的資產並下載相關軟體和 kickstart 檔案的存取權

`ElementalActivationsDownloadSoftwareAccess`是AWS 受管理的策略。

使用此政策

您可以附加`ElementalActivationsDownloadSoftwareAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 9 月 8 日, 世界標準時間 17:26
- 編輯時間：2020 年 9 月 8 日，世界標準時間 17:26
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElementalActivationsFullAccess

描述：完整存取權，可檢視和對元素裝置和軟體購買的資產採取行動

ElementalActivationsFullAccess是AWS 受管理的策略。

使用此政策

您可以附加ElementalActivationsFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 6 月 4 日, 世界標準時間 21:00
- 編輯時間:2020 年 6 月 4 日, 世界標準時間 21:00
- ARN: arn:aws:iam::aws:policy/ElementalActivationsFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElementalActivationsGenerateLicenses

說明：檢視已購買的資產，並產生擱置啟用的軟體授權

ElementalActivationsGenerateLicenses是AWS 受管理的策略。

使用此政策

您可以附加ElementalActivationsGenerateLicenses至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 28 日, 世界標準時間 18:28
- 編輯時間:2020 年 8 月 28 日, 世界標準時間 18:28
- ARN: arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElementalActivationsReadOnlyAccess

描述：與使用者相關聯的已購買資產詳細清單 AWS 帳戶 的唯讀存取權

ElementalActivationsReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加ElementalActivationsReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 8 月 28 日, 世界標準時間 16:51
- 編輯時間:2020 年 8 月 28 日, 世界標準時間 16:51
- ARN: arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElementalAppliancesSoftwareFullAccess

描述：完全訪問權限以查看和對元素設備和軟件報價和訂單採取行動

`ElementalAppliancesSoftwareFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`ElementalAppliancesSoftwareFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 7 月 31 日, 世界標準時間 16:28

- 編輯時間：世界標準時間 2021 年 2 月 5 日晚上 9 時 01 分
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElementalAppliancesSoftwareReadOnlyAccess

描述：檢視 Elemental 設備與軟體報價與訂單的唯讀存取權

`ElementalAppliancesSoftwareReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加ElementalAppliancesSoftwareReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 1 日, 世界標準時間 22:31
- 編輯時間:2020 年 4 月 1 日, 世界標準時間 22:31
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ElementalSupportCenterFullAccess

描述：完整存取權，可檢視 Elemental 裝置和軟體支援案例和產品支援內容並採取行動

ElementalSupportCenterFullAccess是AWS 受管理的策略。

使用此政策

您可以附加ElementalSupportCenterFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年十一月二十五日, 世界標準時間 18:08
- 編輯時間：2021 年 2 月 5 日，世界標準時間 21:02
- ARN: arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

EMRDescribeClusterPolicyForEMRWAL

說明：此政策授予唯讀許可，這些許可允許 Amazon EMR 的 WAL 服務尋找並傳回叢集的狀態

EMRDescribeClusterPolicyForEMRWAL是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 6 月 15 日
- 編輯時間：世界標準時間 2023 年 6 月 15 日 23:30
- ARN: arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

FMSServiceRolePolicy

描述：允許 FM 服務連結角色對客戶組織帳戶內的 FM 管理資源執行與 FM 相關的動作的存取政策。AWS

FMSServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 3 月 28 日, 世界標準時間 23:01
- 編輯時間:2024 年 4 月 22 日, 世界標準時間 19:12
- ARN: arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

政策版本

策略版本：v29(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

FSxDeleteServiceLinkedRoleAccess

說明：允許 Amazon FSx 刪除其服務鏈接角色以進行 Amazon S3 訪問

`FSxDeleteServiceLinkedRoleAccess`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月二十八日, 世界標準時間 10:40
- 編輯時間:2018 年十一月二十八日, 世界標準時間 10:40
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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_*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

GameLiftGameServerGroupPolicy

說明：允許 Gamelift 管理客戶資源 GameServerGroups 的政策

GameLiftGameServerGroupPolicy是AWS 受管理的策略。

使用此政策

您可以附加GameLiftGameServerGroupPolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 4 月 3 日, 23:12 世界標準時間
- 編輯時間:2020 年 5 月 13 日, 世界標準時間 17:27
- ARN: arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:DetachInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sns:Publish",
      "Resource" : [
        "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
        "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

GlobalAcceleratorFullAccess

描述：允許 GlobalAccelerator 使用者完整存取所有 API

GlobalAcceleratorFullAccess是AWS 受管理的策略。

使用此政策

您可以附加GlobalAcceleratorFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 11 月 27 日, 02:44 世界標準時間
- 編輯時間：2020 年 12 月 4 日，世界標準時間 19:17
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

GlobalAcceleratorReadOnlyAccess

說明：允許 GlobalAccelerator 使用者存取唯讀 API

`GlobalAcceleratorReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`GlobalAcceleratorReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 11 月 27 日, 02:41 世界標準時間
- 編輯時間:2018 年十一月二十七日, 02:41 世界標準時間
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

GreengrassOTAUpdateArtifactAccess

說明：提供對所有 Greengrass 區域中 Greengrass OTA 更新成品的讀取存取權

GreengrassOTAUpdateArtifactAccess是AWS 受管理的策略。

使用此政策

您可以附加GreengrassOTAUpdateArtifactAccess至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：2017 年十一月二十九日，世界標準時間 18:11
- 編輯時間：2018 年十二月十八日，世界標準時間 00:59
- ARN: arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
```

```
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

GroundTruthSyntheticConsoleFullAccess

說明：此政策授予使用 G SageMaker round Truth 綜合控制台所有功能所需的權限。

`GroundTruthSyntheticConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`GroundTruthSyntheticConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 25 日，世界標準時間 15:58
- 編輯時間：2022 年 8 月 25 日，世界標準時間 15:58
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

GroundTruthSyntheticConsoleReadOnlyAccess

說明：此原則授予透過 AWS Management Console. SageMaker

GroundTruthSyntheticConsoleReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加GroundTruthSyntheticConsoleReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 8 月 25 日，世界標準時間 15:58
- 編輯時間：2022 年 8 月 25 日，世界標準時間 15:58

- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

Health_OrganizationsServiceRolePolicy

描述：啟用「組織檢視」功能的 AWS Health 政策

`Health_OrganizationsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:二零一九年十二月十六日, 13:28 世界標準
- 編輯時間：世界標準時間 2024 年 2 月 6 日下午 4 時 7 分
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IAMAccessAdvisorReadOnly

說明：此政策授予存取權限，以讀取 IAM 存取建議程式提供的所有存取資訊，例如服務上次存取的資訊。

`IAMAccessAdvisorReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`IAMAccessAdvisorReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 21 日, 世界標準時間 19:33
- 編輯時間：2019 年 6 月 21 日，世界標準時間 19:33
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IAMAccessAnalyzerFullAccess

說明：提供 IAM 存取分析器的完整存取權

IAMAccessAnalyzerFullAccess是AWS 受管理的策略。

使用此政策

您可以附加IAMAccessAnalyzerFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月二日, 17:12 世界標準時
- 編輯時間：2019 年 12 月 2 日，世界標準時間 17:12
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IAMAccessAnalyzerReadOnlyAccess

說明：提供 IAM 存取分析器資源的唯讀存取權

IAMAccessAnalyzerReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加IAMAccessAnalyzerReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一九年十二月二日, 17:12 世界標準時
- 編輯時間：世界標準時間：2023 年 11 月 27 日，下午 2 點 24
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IAMFullAccess

說明：透過提供 IAM 的完整存取權 AWS Management Console。

IAMFullAccess是AWS 受管理的策略。

使用此政策

您可以附加IAMFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間：2019 年 6 月 21 日，世界標準時間 19:40
- ARN: arn:aws:iam::aws:policy/IAMFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IAMReadOnlyAccess

說明：透過 AWS Management Console.

`IAMReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`IAMReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:40 世界標準時間
- 編輯時間:2018 年 1 月 25 日, 世界標準時間 19:11
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IAMSelfManageServiceSpecificCredentials

說明：允許 IAM 使用者管理自己的服務特定登入資料。

IAMSelfManageServiceSpecificCredentials是AWS 受管理的策略。

使用此政策

您可以附加IAMSelfManageServiceSpecificCredentials至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零一六年十二月二十二日, 下午 17 點 25
- 編輯時間：二零一六年十二月二十二日下午 17 時 25 分
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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}"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制

- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IAMUserChangePassword

說明：提供 IAM 使用者變更自己密碼的功能。

IAMUserChangePassword是AWS 受管理的策略。

使用此政策

您可以附加IAMUserChangePassword至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二零一六年十一月十五日凌空 00:25
- 編輯時間：二零一六年十一月十五日 23:18 世界標準時
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IAMUserSSHKeys

說明：提供 IAM 使用者管理自己的安全殼層金鑰的功能。

IAMUserSSHKeys是AWS 受管理的策略。

使用此政策

您可以附加IAMUserSSHKeys至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 7 月 9 日, 世界標準時間 17:08
- 編輯時間:2015 年 7 月 9 日, 世界標準時間 17:08
- ARN: arn:aws:iam::aws:policy/IAMUserSSHKeys

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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}"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IVSFullAccess

描述：提供完整存取互動式視訊服務 (IVS) 的完整存取權，也包含完整存取 ivs 主控台所需的相依服務權限。

IVSFullAccess是AWS 受管理的策略。

使用此政策

您可以附加IVSFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:二零二一年十二月十三日, 21:20 世界標準時間
- 編輯時間：世界標準時間 2023 年 12 月 13 日晚上 9 點 20 分
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IVSReadOnlyAccess

說明：提供 IVS 低延遲和即時串流 API 的唯讀存取

IVSReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加IVSReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 2023 年 12 月 5 日下午 6 點
- 編輯時間：世界標準時間 2024 年 2 月 16 日下午 18:03
- ARN: arn:aws:iam::aws:policy/IVSReadOnlyAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

IVSRecordToS3

說明：執行 S3 以記錄 IVS 即時串流 PutObject 的服務連結角色

IVSRecordToS3是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2020 年十二月 5 日，世界標準時間 00:10
- 編輯時間：2020 年十二月 5 日，世界標準時間 00:10
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

KafkaConnectServiceRolePolicy

說明：此政策授予 Kafka Connect 代表您管理 AWS 資源的權限。

KafkaConnectServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 9 月 7 日, 世界標準時間 13:12
- 編輯時間：2021 年 9 月 7 日，世界標準時間 13:12
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

KafkaServiceRolePolicy

說明：適用於卡夫卡的 IAM 服務連結角色政策。

KafkaServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年十一月十五日, 23:31 世界標準時間
- 編輯時間:2023 年 4 月 28 日, 00:39 世界標準時間
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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_*"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

KeyspacesReplicationServiceRolePolicy

說明：跨區域資料複寫所需的 Keyspaces 權限

`KeyspacesReplicationServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2023 年 5 月 2 日, 16:15 世界標準時間
- 編輯時間:2023 年 5 月 2 日, 世界標準時間 16:15
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

LakeFormationDataAccessServiceRolePolicy

描述：授予對 Lake Formation 資源的臨時數據訪問權限的政策

`LakeFormationDataAccessServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 6 月 20 日, 世界標準時間 20:46
- 編輯時間：世界標準時間 2024 年 2 月 6 日下午 18:37

- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

LexBotPolicy

說明： AWS Lex Bot 使用案例的政策

`LexBotPolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 2 月 17 日, 世界標準時間 22:18
- 編輯時間：2019 年十一月十三日，世界標準時間 22:29
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

LexChannelPolicy

說明： AWS Lex 頻道使用案例的政策

LexChannelPolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2017 年 2 月 17 日, 世界標準時間 23:23
- 編輯時間：2017 年 2 月 17 日，世界標準時間 23:23
- ARN: arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

LightsailExportAccess

說明：授與匯出資源權限的 AWS Lightsail 服務連結角色原則

`LightsailExportAccess`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 9 月 28 日, 世界標準時間 16:35
- 編輯時間:2022 年 1 月 15 日, 世界標準時間 1:45
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

MediaConnectGatewayInstanceRolePolicy

說明：此政策授與將 MediaConnect 閘道執行個體註冊至 MediaConnect 閘道的權限。

MediaConnectGatewayInstanceRolePolicy是AWS 受管理的策略。

使用此政策

您可以附加MediaConnectGatewayInstanceRolePolicy至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:世界標準時間 2023 年 3 月 22 日, 20:43
- 編輯時間：世界標準時間 2023 年 3 月 22 日 , 20:43
- ARN: arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

MediaPackageServiceRolePolicy

描述：允許 MediaPackage 將記錄檔發佈到 CloudWatch

`MediaPackageServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2020 年 9 月 18 日, 世界標準時間 17:45
- 編輯時間:2020 年 9 月 18 日, 世界標準時間 17:45
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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/*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

MemoryDBServiceRolePolicy

描述：此原則允許 MemoryDB 在必要時代表您管理 AWS 資源來管理資源。

MemoryDBServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2021 年 8 月 17 日, 世界標準時間 22:34
- 編輯時間:2021 年 8 月 18 日, 世界標準時間 23:48

- ARN: arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
```

```
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

MigrationHubDMSAccessServiceRolePolicy

說明：資 Database Migration Service 在客戶帳戶中扮演角色以呼叫 Migration Hub 的原則

`MigrationHubDMSAccessServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 6 月 12 日, 世界標準時間 17:50
- 編輯時間:2019 年 10 月 7 日, 世界標準時間 17:57
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

MigrationHubServiceRolePolicy

描述：允許 Migration Hub 代表您呼叫 Application Discovery Service

`MigrationHubServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 6 月 12 日, 世界標準時間 17:22
- 編輯時間:2020 年 8 月 6 日, 世界標準時間 18:08
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

MigrationHubSMSAccessServiceRolePolicy

說明：伺服器移轉服務在客戶帳戶中扮演角色以呼叫 Migration Hub 的政策

`MigrationHubSMSAccessServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 6 月 12 日, 世界標準時間 18:30
- 編輯時間:2019 年 10 月 7 日, 世界標準時間 18:02
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

MonitronServiceRolePolicy

描述：授與所需客戶資源存取權的 AWS Monitron 服務連結角色的政策。

MonitronServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2022 年 5 月 2 日, 世界標準時間 19:22
- 編輯時間：2022 年 5 月 2 日，世界標準時間 19:22
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

NeptuneConsoleFullAccess

說明：提供完整的存取權，以便使用 AWS Management Console. 請注意，此政策還授予在帳戶內所有 SNS 主題上發佈的完整存取權、建立和編輯 Amazon EC2 執行個體和 VPC 組態的許可、在 Amazon KMS 上檢視和列出金鑰的許可，以及對 Amazon RDS 的完整存取權。如需詳細資訊，請參閱 https://aws.amazon.com/neptune/faqs/。

NeptuneConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加NeptuneConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 6 月 19 日, 世界標準時間 21:35
- 編輯時間：世界標準時間：2023 年 11 月 30 日上午 07 時 32 分
- ARN: arn:aws:iam::aws:policy/NeptuneConsoleFullAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
```

```
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
```

```
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
```

```
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
```

```
        "ec2:ModifyVpcEndpoint",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : [
```

```
        "neptune-graph:CreateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:GetGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:UpdateGraph",
        "neptune-graph:ResetGraph",
        "neptune-graph:CreateGraphSnapshot",
        "neptune-graph:DeleteGraphSnapshot",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:RestoreGraphFromSnapshot",
        "neptune-graph:CreatePrivateGraphEndpoint",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:DeletePrivateGraphEndpoint",
        "neptune-graph:CreateGraphUsingImportTask",
        "neptune-graph:GetImportTask",
        "neptune-graph:ListImportTasks",
        "neptune-graph:CancelImportTask"
      ],
      "Resource" : [
        "arn:aws:neptune-graph:*:*:*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "neptune-graph.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "neptune-graph.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

NeptuneFullAccess

描述：提供對 Amazon Neptune 的完整存取權。請注意，此政策還授予對帳戶內所有 SNS 主題進行發佈的完整存取權，以及對 Amazon RDS 的完整存取權。如需詳細資訊，請參閱 https://aws.amazon.com/neptune/faqs/。

`NeptuneFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`NeptuneFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 30 日, 世界標準時間 19:17
- 編輯時間：世界標準時間 2024 年 1 月 22 日下午 16:32
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterEndpoint",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
```

```
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:FailoverGlobalCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
```

```
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:StartDBCluster",
        "rds:StopDBCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDataAccessForNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集

- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

NeptuneGraphReadOnlyAccess

描述：提供對所有 Amazon Neptune 分析資源的唯讀存取權限，以及相依服務的唯讀權限。

NeptuneGraphReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加NeptuneGraphReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：2023 年 11 月 30 日上午 07 時 32 分
- 編輯時間：世界標準時間：2023 年 11 月 30 日上午 07 時 32 分
- ARN: arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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:*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

NeptuneReadOnlyAccess

描述：提供對 Amazon Neptune 的唯讀存取。請注意，此政策也會授予對 Amazon RDS 資源的存取權。如需詳細資訊，請參閱 https://aws.amazon.com/neptune/faqs/。

`NeptuneReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`NeptuneReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 5 月 30 日, 世界標準時間 19:16
- 編輯時間：世界標準時間 2024 年 1 月 22 日下午 16:33
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

NetworkAdministrator

描述：授予對設定和設定 AWS 網路資源所需之 AWS 服務和動作的完整存取權限。

NetworkAdministrator是AWS 受管理的策略。

使用此政策

您可以附加NetworkAdministrator至您的使用者、群組和角色。

政策詳情

- 類型：Job 職能政策
- 創建時間：二零一六年十一月十日 17:31 世界標準時間
- 編輯時間：2021 年 9 月 16 日，世界標準時間 20:22
- ARN: arn:aws:iam::aws:policy/job-function/NetworkAdministrator

政策版本

策略版本：v11(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

OAMFullAccess

描述：提供對 CloudWatch 觀察性存取管理員的完整存取權

OAMFullAccess是AWS 受管理的策略。

使用此政策

您可以附加OAMFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：二○二○二年十一月二十七日，下午 13:38
- 編輯時間：2022 年十一月二十七日，世界標準時間 13:38
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

OAMReadOnlyAccess

描述：提供 CloudWatch 觀測性存取管理員的唯讀存取權

OAMReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加OAMReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間：二零二年十一月二十七日
- 編輯時間：2022 年十一月二十七日，世界標準時間下午
- ARN: arn:aws:iam::aws:policy/OAMReadOnlyAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

PartnerCentralAccountManagementUserRoleAssociation

說明：提供將合作夥伴中央使用者與 IAM 角色建立關聯和分離的存取權

`PartnerCentralAccountManagementUserRoleAssociation`是AWS 受管理的策略。

使用此政策

您可以附加`PartnerCentralAccountManagementUserRoleAssociation`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間十一月十日（世界標準時間）
- 編輯時間：世界標準時間：2023 年 11 月 10 日，02:03
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

PowerUserAccess

描述：提供對 AWS 服務和資源的完整存取權，但不允許管理使用者和群組。

PowerUserAccess是AWS 受管理的策略。

使用此政策

您可以附加PowerUserAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間:世界標準時間 2023 年 7 月 6 日, 22:04
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

QBusinessServiceRolePolicy

說明：授予 Amazon Q 使用或管理的許可 AWS 服務 和資源

QBusinessServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 4 月 29 日, 世界標準時間 16:05
- 編輯時間：世界標準時間 2024 年 4 月 29 日，16:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QBusiness"
        }
      }
    },
    {
      "Sid" : "QBusinessCreateLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessDescribeLogGroupsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "QBusinessLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

說明： QuickSight 團隊用來存取 S3 儲存管理分析產生的客戶資料的政策。

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2017 年 6 月 12 日, 世界標準時間 18:18
- 編輯時間：2019 年 10 月 8 日，世界標準時間 23:53
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

RDSCloudHsmAuthorizationRole

說明：Amazon RDS 服務角色的預設政策。

RDSCloudHsmAuthorizationRole是AWS 受管理的策略。

使用此政策

您可以附加RDSCloudHsmAuthorizationRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2019 年 9 月 26 日，世界標準時間 22:14
- ARN: arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ReadOnlyAccess

描述：提供 AWS 服務和資源的唯讀存取權。

ReadOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加ReadOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間：世界標準時間 2024 年 4 月 17 日 21:17
- ARN: arn:aws:iam::aws:policy/ReadOnlyAccess

政策版本

策略版本：v112(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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",
        "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:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
```

```
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
```

```
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "sagemaker-groundtruth-synthetic:GetAccountDetails",
        "sagemaker-groundtruth-synthetic:GetBatch",
        "sagemaker-groundtruth-synthetic:GetProject",
        "sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
        "sagemaker-groundtruth-synthetic:ListBatchSummaries",
        "sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
        "sagemaker-groundtruth-synthetic:ListProjectSummaries",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
```

```
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "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",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
```

```
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCases",
```

```
        "support:DescribeCommunications",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "sustainability:GetCarbonFootprintSummary",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
```

```
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
```

```
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:ListAnswers",
        "wellarchitected:ListCheckDetails",
        "wellarchitected:ListCheckSummaries",
        "wellarchitected:ListLenses",
        "wellarchitected:ListLensReviewImprovements",
        "wellarchitected:ListLensReviews",
        "wellarchitected:ListLensShares",
        "wellarchitected:ListMilestones",
        "wellarchitected:ListNotifications",
        "wellarchitected:ListProfileNotifications",
        "wellarchitected:ListProfiles",
        "wellarchitected:ListProfileShares",
        "wellarchitected:ListReviewTemplateAnswers",
        "wellarchitected:ListReviewTemplates",
        "wellarchitected:ListShareInvitations",
        "wellarchitected:ListTagsForResource",
        "wellarchitected:ListTemplateShares",
        "wellarchitected:ListWorkloads",
```

```
        "wellarchitected:ListWorkloadShares",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ResourceGroupsandTagEditorFullAccess

描述：提供對 Resource Groups 和標籤編輯器的完整存取權。

ResourceGroupsandTagEditorFullAccess是AWS 受管理的策略。

使用此政策

您可以附加ResourceGroupsandTagEditorFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間：世界標準時間 2023 年 8 月 10 日，13:29
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ResourceGroupsandTagEditorReadOnlyAccess

描述：提供使用 Resource Groups 和標籤編輯器的存取權，但不允許透過標籤編輯器編輯標籤。

`ResourceGroupsandTagEditorReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`ResourceGroupsandTagEditorReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 18:39 世界標準時間
- 編輯時間:2023 年 8 月 10 日, 世界標準時間 13:42
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ResourceGroupsServiceRolePolicy

描述：允許 AWS Resource Groups 查詢擁有您資源的 AWS 服務，以保留群組 up-to-date

`ResourceGroupsServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間 2023 年 1 月 5 日, 16:57
- 編輯時間：世界標準時間 2023 年 1 月 5 日，16:57
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAAmazonEBSCSIDriverOperatorPolicy

描述：允許 OpenShift Amazon EBS 容器儲存介面 (CSI) 驅動程式操作員在紅帽 OpenShift 服務 AWS (ROSA) 叢集上安裝和維護 Amazon EBS CSI 驅動程式。Amazon EBS CSI 驅動程式可讓 ROSA 叢集管理持續性磁碟區的 Amazon EBS 磁碟區的生命週期。

ROSAAmazonEBSCSIDriverOperatorPolicy是AWS 受管理的策略。

使用此政策

您可以附加ROSAAmazonEBSCSIDriverOperatorPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2023 年 4 月 20 日, 世界標準時間 22:36
- 編輯時間:世界標準時間 2023 年 4 月 20 日, 22:36
- ARN: arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSACloudNetworkConfigOperatorPolicy

描述：允許 OpenShift 雲端網路 Config 控制器操作員佈建和管理網路資源，以供 Red Hat OpenShift Service on AWS (ROSA) 叢集網路覆蓋使用。 OpenShift 雲網絡運營商通過代表網絡插件與 AWS API 接口 CustomResourceDefinitions. 操作員使用這些政策許可來管理 Amazon EC2 執行個體的私有 IP 地址，做為 ROSA 叢集的一部分。

ROSACloudNetworkConfigOperatorPolicy是AWS 受管理的策略。

使用此政策

您可以附加ROSACloudNetworkConfigOperatorPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 4 月 20 日, 世界標準時間 22:34
- 編輯時間:世界標準時間 2023 年 4 月 20 日, 22:34
- ARN: arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAControlPlaneOperatorPolicy

描述：允許紅帽 OpenShift 服務 AWS (ROSA) 控制平面管理 ROSA 叢集 Amazon EC2 和 Amazon Route 53 資源。

ROSAControlPlaneOperatorPolicy是AWS 受管理的策略。

使用此政策

您可以附加ROSAControlPlaneOperatorPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 4 月 24 日, 世界標準時間 23:02
- 編輯時間：世界標準時間 2023 年 6 月 30 日晚上 9 時 12 分
- ARN: arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAImageRegistryOperatorPolicy

說明：允許 OpenShift 映像登錄操作員佈建和管理 Amazon S3 儲存貯體和物件，以供 Red Hat OpenShift 服務 AWS (ROSA) 叢集內映像登錄使用，以滿足 ROSA 儲存需求。映 OpenShift 像登錄操作員會安裝並維護 Red Hat OpenShift 叢集的內部登錄。

`ROSAImageRegistryOperatorPolicy`是AWS 受管理的策略。

使用此政策

您可以附加ROSAImageRegistryOperatorPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 4 月 27 日, 世界標準時間 20:13
- 編輯時間：世界標準時間 2023 年 12 月 12 日，下午 19:53
- ARN: arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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}/*"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAIngressOperatorPolicy

描述：允許 OpenShift 入口操作員佈建及管理 Red Hat OpenShift 服務 (ROSA) 叢集上的負載平衡器和網域名稱系統 AWS (DNS) 組態。此原則允許對標籤值進行讀取存取，操作員會篩選 Route 53 資源以探索託管區域。

ROSAIngressOperatorPolicy是AWS 受管理的策略。

使用此政策

您可以附加ROSAIngressOperatorPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2023 年 4 月 20 日, 世界標準時間 22:37
- 編輯時間:世界標準時間 2023 年 4 月 20 日, 22:37
- ARN: arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAInstallerPolicy

描述：允許在 AWS (ROSA) 安裝程式上的 Red Hat OpenShift 服務管理支援 ROSA 叢集安裝的 AWS 資源。這包括管理 ROSA 工作者節點的執行個體設定檔。

ROSAInstallerPolicy是AWS 受管理的策略。

使用此政策

您可以附加ROSAInstallerPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:世界標準時間 6 月 6 日晚上 9 點
- 編輯時間：世界標準時間 2024 年 4 月 24 日，19:49
- ARN: arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAKMSProviderPolicy

說明：允許內建 ROSA AWS 加密提供者管理金 AWS 鑰管理服務 (KMS) 金鑰，以支援使用客戶提供的 AWS KMS 金鑰進行 etcd 資料加密。此原則允許使用 KMS 金鑰加密和解密資料。

ROSAKMSProviderPolicy是AWS 受管理的策略。

使用此政策

您可以附加ROSAKMSProviderPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零二一年四月二十七日, 世界標準時間 20:10
- 編輯時間：世界標準時間 2023 年 4 月 27 日晚上 20:10
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAKubeControllerPolicy

描述：允許 ROSA Kubernetes 控制器管理 ROSA 叢集的 Amazon EC2、Elastic Load Balancing (ELB) 和金 AWS 鑰管理服務 (KMS) 資源。

ROSAKubeControllerPolicy是AWS 受管理的策略。

使用此政策

您可以附加ROSAKubeControllerPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:二零二一年四月二十七日, 世界標準時間 20:09
- 編輯時間:世界標準時間 2023 年 10 月 16 日, 18:17
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagementResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateListeners",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true",
```

```
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateLoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ModifySecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAManageSubscription

描述：此原則提供管理 Red Hat OpenShift 服務 AWS (ROSA) 訂閱所需的權限。

ROSAManageSubscription是AWS 受管理的策略。

使用此政策

您可以附加ROSAManageSubscription至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2022 年 4 月 11 日，世界標準時間 20:58
- 編輯時間:2023 年 8 月 4 日, 世界標準時間 19:59
- ARN: arn:aws:iam::aws:policy/ROSAManageSubscription

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSANodePoolManagementPolicy

說明：允許 Red Hat OpenShift 服務 AWS (ROSA) 將叢集 EC2 執行個體當做工作者節點來管理，包括設定安全群組和標記執行個體和磁碟區的權限。此政策也允許透過金鑰管理服務 (KMS) 金鑰提供的 AWS 磁碟加密使用 EC2 執行個體。

`ROSANodePoolManagementPolicy`是AWS 受管理的策略。

使用此政策

您可以附加`ROSANodePoolManagementPolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2023 年 6 月 8 日, 世界標準時間 20:48
- 編輯時間:2024 年 5 月 2 日, 世界標準時間 14:01

- ARN: arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSASRESupportPolicy

描述：提供 ROSA 站台可靠性工程 (SRE) 所需的權限，以便初始觀察、診斷及支援與 Red Hat OpenShift 服務 AWS (ROSA) 叢集相關的 AWS 資源，包括變更 ROSA 叢集節點狀態的能力。

ROSASRESupportPolicy是AWS 受管理的策略。

使用此政策

您可以附加ROSASRESupportPolicy至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間：世界標準時間 6 月 1 日，下午 2:36
- 編輯時間：世界標準時間 2024 年 4 月 10 日晚上 20:51
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "VPCNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudtrail",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "DescribeLoadBalancers",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DescribeAddressesAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeAddressesAttribute",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
    },
    {
      "Sid" : "DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageInstanceLifecycle",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ROSAWorkerInstancePolicy

說明：允許您帳戶中 AWS (ROSA) 工作者節點上的 Red Hat OpenShift 服務以唯讀方式存取 Amazon EC2 執行個體和 AWS 區域 運算節點生命週期管理。

`ROSAWorkerInstancePolicy`是AWS 受管理的策略。

使用此政策

您可以附加`ROSAWorkerInstancePolicy`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2023 年 4 月 20 日, 世界標準時間 22:35
- 編輯時間:世界標準時間 2023 年 4 月 20 日, 22:35

- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

Route53RecoveryReadinessServiceRolePolicy

說明：Route 53 復原準備的服務連結角色原則

`Route53RecoveryReadinessServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:世界標準時間 7 月 15 日, 16:06
- 編輯時間：世界標準時間 2023 年 2 月 14 日下午 18:08
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

Route53ResolverServiceRolePolicy

描述：啟用 Route53 解析器使用或管理的資源的存取 AWS 服務 和資源

Route53ResolverServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 8 月 12 日, 世界標準時間 17:47
- 編輯時間:2020 年 8 月 12 日, 世界標準時間 17:47
- ARN: arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

S3StorageLensServiceRolePolicy

說明：可存取 AWS 服務 S3 儲存鏡頭所使用或管理的資源

`S3StorageLensServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年十一月十八日, 世界標準時間 18:15
- 編輯時間:2020 年十一月十八日, 世界標準時間 18:15
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

SecretsManagerReadWrite

說明：透過提供對 AWS Secrets Manager 的讀取/寫入存取權 AWS Management Console。附註：這會排除 IAM 動作，因此FullAccess 如果需要輪換組態，請與 IAM 結合使用。

`SecretsManagerReadWrite`是AWS 受管理的策略。

使用此政策

您可以附加SecretsManagerReadWrite至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年 4 月 4 日, 18:05 世界標準時間
- 編輯時間：世界標準時間 2024 年 2 月 22 日下午 18 時 12 分
- ARN: arn:aws:iam::aws:policy/SecretsManagerReadWrite

政策版本

策略版本：v5(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
```

```
        "kms:ListKeys",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
    },
    {
      "Sid" : "SARPermissions",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:CreateCloudFormationChangeSet",
        "serverlessrepo:GetApplication"
      ],
      "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
    },
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo-changesets*",
        "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

SecurityAudit

描述：安全性稽核範本會授與讀取安全性組態中繼資料的存取權。這對於稽核組態的軟體非常有用 AWS 帳戶。

SecurityAudit是AWS 受管理的策略。

使用此政策

您可以附加SecurityAudit至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：世界標準時間 2024 年 4 月 5 日下午 17 時 32 分
- ARN: arn:aws:iam::aws:policy/SecurityAudit

政策版本

策略版本：v42(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
```

```
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3: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"
      ]
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

SecurityLakeServiceLinkedRole

說明：此政策授予代表您操作 Amazon 安全湖服務的許可

`SecurityLakeServiceLinkedRole`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：世界標準時間：二零二二年十一月二十九
- 編輯時間：世界標準時間 2024 年 4 月 19 日 16:00
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

政策版本

策略版本：v3(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
```

```
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ServerMigration_ServiceRole

說明：允許 AWS 伺服器遷移服務將 VM 遷移到 EC2 的許可：允許伺服器遷移服務將遷移的資源放入客戶的 EC2 帳戶。

ServerMigration_ServiceRole是AWS 受管理的策略。

使用此政策

您可以附加ServerMigration_ServiceRole至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 8 月 11 日, 世界標準時間 20:41
- 編輯時間:2020 年 10 月 15 日, 世界標準時間 17:26
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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-*/*"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ServerMigrationConnector

說明：允許 AWS 伺服器移轉連接器將虛擬機器移轉至 EC2 的權限。允許與 AWS 伺服器遷移服務通訊、以 'sms-b-' 和 'import-to-ec2-' 開始對 S3 儲存貯體的讀取/寫入存取，以及用於伺服器遷移連接器升級的儲存貯體、 AWS AWS 伺服器遷移連接器註冊以及指標上傳至。 AWS AWS

`ServerMigrationConnector`是AWS 受管理的策略。

使用此政策

您可以附加`ServerMigrationConnector`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:十月二十四日, 世界標準時間 21:45
- 編輯時間：2016 年 10 月 24 日，世界標準時間 21:45
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ServerMigrationServiceConsoleFullAccess

說明：使用伺服器移轉服務主控台所有功能的必要權限

ServerMigrationServiceConsoleFullAccess是AWS 受管理的策略。

使用此政策

您可以附加ServerMigrationServiceConsoleFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2020 年 5 月 9 日, 世界標準時間 17:18
- 編輯時間：世界標準時間 7 月 20 日晚上 10 點
- ARN: arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
```

```
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ServerMigrationServiceLaunchRole

說明：允許伺服 AWS 器移轉服務建立並更新客戶相關 AWS 資源以啟動已移轉伺服器和應用程式的權限。 AWS 帳戶

`ServerMigrationServiceLaunchRole`是AWS 受管理的策略。

使用此政策

您可以附加`ServerMigrationServiceLaunchRole`至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2018 年十一月二十六日, 世界標準時間 19:53
- 編輯時間:2020 年 10 月 15 日, 世界標準時間 17:29
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ServerMigrationServiceRoleForInstanceValidation

說明：允許 AWS SMS 執行使用的資料驗證指令碼，並將指令碼成功/失敗傳送回 SMS 的權限

ServerMigrationServiceRoleForInstanceValidation是AWS 受管理的策略。

使用此政策

您可以附加ServerMigrationServiceRoleForInstanceValidation至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2020 年 7 月 20 日, 世界標準時間 22:25
- 編輯時間:2020 年 7 月 20 日, 世界標準時間 22:25
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ServiceQuotasFullAccess

說明：提供 Service Quotas 的完整存取權

`ServiceQuotasFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`ServiceQuotasFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 6 月 24 日, 世界標準時間 15:44
- 編輯時間：世界標準時間 2021 年 2 月 4 日晚上 9 時 29 分
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

政策版本

策略版本：v4(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ServiceQuotasReadOnlyAccess

說明：提供 Service Quotas 的唯讀存取權

`ServiceQuotasReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`ServiceQuotasReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- **創建時間:**2019 年 6 月 24 日, 世界標準時間 15:31
- **編輯時間:**2020 年十二月二十一日, 世界標準時間 18:11
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ServiceQuotasServiceRolePolicy

說明：允許 Service Quotas 代表您建立支援案例

`ServiceQuotasServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2019 年 5 月 22 日, 世界標準時間 20:44
- 編輯時間：2019 年 6 月 24 日，世界標準時間 14:52
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

SimpleWorkflowFullAccess

描述：提供「簡單工作流程」組態服務的完整存取權。

SimpleWorkflowFullAccess是AWS 受管理的策略。

使用此政策

您可以附加SimpleWorkflowFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略

- 創建時間:2015 年 2 月 6 日, 世界標準時間 18:41
- 編輯時間：2015 年 2 月 6 日，世界標準時間 18:41
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

SplitCostAllocationDataServiceRolePolicy

描述：允許分割成本配置資料擷取 Organ AWS izations 資訊 (如果適用)，並針對客戶選擇加入的分割成本配置資料服務收集遙測資料。

SplitCostAllocationDataServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2020 年 4 月 16 日, 世界標準時間 16:05
- 編輯時間：世界標準時間 2024 年 4 月 16 日，16:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

SupportUser

說明：此原則授與疑難排解和解決 AWS 帳戶. 此原則也可讓使用者與 AWS 支援人員聯絡，以建立和管理案例。

SupportUser是AWS 受管理的策略。

使用此政策

您可以附加SupportUser至您的使用者、群組和角色。

政策詳情

- 類型：Job 職能政策
- 創建時間：二零一六年十一月十日 17:21 世界標準時間
- 編輯時間:2023 年 8 月 25 日, 世界標準時間 18:40
- ARN: arn:aws:iam::aws:policy/job-function/SupportUser

政策版本

策略版本：v8(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

SystemAdministrator

描述：授予應用程式和開發作業所需資源所需的完整存取權限。

SystemAdministrator是AWS 受管理的策略。

使用此政策

您可以附加SystemAdministrator至您的使用者、群組和角色。

政策詳情

- 類型：Job 職能政策
- 創建時間:二零一六年十一月十日, 17:23 世界標準時
- 編輯時間：2020 年 8 月 24 日，世界標準時間 20:05
- ARN: arn:aws:iam::aws:policy/job-function/SystemAdministrator

政策版本

策略版本：v6(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
```

```
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
```

```
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
```

```
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2:Import*",
        "ec2:Modify*",
        "ec2:MonitorInstances",
        "ec2:MoveAddressToVpc",
        "ec2:Purchase*",
        "ec2:RegisterImage",
        "ec2:Release*",
        "ec2:Replace*",
        "ec2:ReportInstanceStatus",
        "ec2:Request*",
        "ec2:Reset*",
        "ec2:RestoreAddressToClassic",
        "ec2:RunScheduledInstances",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnmonitorInstances",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticloadbalancing:*",
        "events:*",
        "iam:GetAccount*",
        "iam:GetContextKeys*",
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
```

```
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
```

```
        "ec2:RebootInstances",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "s3:*",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetAccessKeyLastUsed",
        "iam:GetGroup*",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy*",
        "iam:GetRole*",
        "iam:GetSAMLProvider",
        "iam:GetSSHPublicKey",
        "iam:GetServerCertificate",
        "iam:GetServiceLastAccessed*",
        "iam:GetUser*",
        "iam:ListAccessKeys",
        "iam:ListAttached*",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles*",
        "iam:ListMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
```

```
        "iam:ListSSHPublicKeys",
        "iam:ListSigningCertificates",
        "iam:ListUserPolicies",
        "iam:Upload*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

TranslateFullAccess

描述：提供對 Amazon Translate 的完整訪問權限。

`TranslateFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加TranslateFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十七日, 世界標準時間 23:36
- 編輯時間:2020 年 1 月 8 日, 世界標準時間 21:22
- ARN: arn:aws:iam::aws:policy/TranslateFullAccess

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

TranslateReadOnly

說明：提供 Amazon Translate 的唯讀存取權。

`TranslateReadOnly`是AWS 受管理的策略。

使用此政策

您可以附加`TranslateReadOnly`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：2017 年十一月二十九日，世界標準時間 18:22
- 編輯時間:世界標準時間 5 月 24 日, 下午 17 時 19 分
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

政策版本

策略版本：v7(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

ViewOnlyAccess

說明：此原則授與檢視所有 AWS 服務之資源和基本中繼資料的權限。

ViewOnlyAccess是AWS 受管理的策略。

使用此政策

您可以附加ViewOnlyAccess至您的使用者、群組和角色。

政策詳情

- 類型：Job 職能政策
- 創建時間:二零一六年十一月十日, 17 世界標準時間

- **編輯時間**：世界標準時間 2024 年 3 月 28 日 21:28
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

政策版本

策略版本：v18(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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: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"
      ]
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

VMImportExportRoleForAWSConnector

描述：針對使用連接器的客戶，虛擬機 AWS 器匯入/匯出服務角色的預設原則。虛擬機器匯入/匯出服務會擔任此原則的角色，以滿足來自連接器虛擬應用裝置的虛擬機 AWS 器移轉要求。(請注意， AWS 連接器會使用 "AWSConnector" 受管理的原則，代表客戶向虛擬機器匯入/匯出服務發出要求。) 提供建立 AMI 和 EBS 快照、修改 EBS 快照屬性、在 EC2 物件上進行「描述 *」呼叫，以及從 S3 儲存貯體讀取「2」開始的功能。import-to-ec

VMImportExportRoleForAWSConnector是AWS 受管理的策略。

使用此政策

您可以附加VMImportExportRoleForAWSConnector至您的使用者、群組和角色。

政策詳情

- 類型：服務角色策略
- 創建時間:2015 年 9 月 3 日, 世界標準時間 20:48
- 編輯時間：2015 年 9 月 3 日，世界標準時間 20:48
- ARN: arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有該策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

VPCLatticeFullAccess

描述：提供對 Amazon VPC 萊迪思的完整存取權限，以及相依性服務的存取權。

VPCLatticeFullAccess是AWS 受管理的策略。

使用此政策

您可以附加VPCLatticeFullAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 3 月 30 日，下午 2 時 49 分
- 編輯時間：世界標準時間 2023 年 3 月 30 日，02:49
- ARN: arn:aws:iam::aws:policy/VPCLatticeFullAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

VPCLatticeReadOnlyAccess

說明：透過相依性服務和有限存取權限 AWS Management Console，提供 Amazon VPC Laters 的唯讀存取權。

`VPCLatticeReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`VPCLatticeReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 3 月 30 日，下午 2 時 47 分
- 編輯時間：世界標準時間 2023 年 3 月 30 日，02:47
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

VPCLatticeServicesInvokeAccess

說明：提供叫用 Amazon VPC 萊迪思服務的存取權。

VPCLatticeServicesInvokeAccess是AWS 受管理的策略。

使用此政策

您可以附加VPCLatticeServicesInvokeAccess至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間：世界標準時間 3 月 30 日，下午 2 時 45 分
- 編輯時間：世界標準時間 2023 年 3 月 30 日，02:45
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

WAFLoggingServiceRolePolicy

說明：建立 SLR 以將客戶的記錄寫入防火器串流

WAFLoggingServiceRolePolicy是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 8 月 24 日, 世界標準時間 21:05
- 編輯時間:2018 年 8 月 24 日, 世界標準時間 21:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
```

```
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

WAFRegionalLoggingServiceRolePolicy

說明：建立 SLR 以將客戶的記錄寫入防火器串流

`WAFRegionalLoggingServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間:2018 年 8 月 24 日, 18:40 世界標準時間
- 編輯時間:2018 年 8 月 24 日, 世界標準時間 18:40
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

WAFV2LoggingServiceRolePolicy

說明：此政策會建立服務連結角色，讓 AWS WAF 將日誌寫入 Amazon Kinesis Data Firehose。

`WAFV2LoggingServiceRolePolicy`是AWS 受管理的策略。

使用此政策

此原則附加至服務連結角色，可讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳情

- 類型：服務連結角色原則
- 創建時間：2019 年 11 月 7 日，世界標準時間 00:40
- 編輯時間:2020 年 7 月 23 日, 世界標準時間 17:04

- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

WellArchitectedConsoleFullAccess

說明：提供完整存取 AWS Well-Architected 的工具，透過 AWS Management Console

`WellArchitectedConsoleFullAccess`是AWS 受管理的策略。

使用此政策

您可以附加`WellArchitectedConsoleFullAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十九日, 世界標準時間 18:19
- 編輯時間:2018 年十一月二十九日, 世界標準時間 18:19
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

WellArchitectedConsoleReadOnlyAccess

說明：透過以唯讀方式存取 AWS Well-Architected 的工具 AWS Management Console

`WellArchitectedConsoleReadOnlyAccess`是AWS 受管理的策略。

使用此政策

您可以附加`WellArchitectedConsoleReadOnlyAccess`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2018 年十一月二十九日, 世界標準時間 18:21
- 編輯時間:世界標準時間 6 月 29 日, 下午 17 時 16 分
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

政策版本

策略版本：v2(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

WorkLinkServiceRolePolicy

說明：啟用 Amazon 所使用或管理的資源存取 AWS 服務 和資源 WorkLink

`WorkLinkServiceRolePolicy`是AWS 受管理的策略。

使用此政策

您可以附加`WorkLinkServiceRolePolicy`至您的使用者、群組和角色。

政策詳情

- 類型： AWS 受管理的策略
- 創建時間:2019 年 1 月 23 日, 世界標準時間 19:03
- 編輯時間：2019 年 1 月 23 日，世界標準時間 19:03
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

政策版本

策略版本：v1(預設值)

原則的預設版本是定義原則權限的版本。當具有策略的使用者或角色發出要求以存取 AWS 資源時，請 AWS 檢查原則的預設版本，以決定是否允許該要求。

政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 使用 IAM 身分中心的 AWS 受管政策建立權限集
- 新增和移除 IAM 身分許可
- 瞭解 IAM 政策的版本控制
- 開始使用 AWS 受管理的原則，並邁向最低權限權限

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。