Referenzhandbuch

AWS Verwaltete Richtlinie

AWS Verwaltete Richtlinie: Referenzhandbuch

Table of Contents

Was sind -AWSverwaltete Richtlinien?

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wirdAWS. AWS Von verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele häufige Anwendungsfälle bereitstellen. Sie erleichtern Ihnen den Einstieg in die Zuweisung von Berechtigungen für Benutzer, Gruppen und Rollen, als ob Sie die Richtlinien selbst schreiben müssten.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise keine Berechtigungen mit den geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich die Aktualisierung auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für vorhandene Services verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Grundlegendes zu Richtlinienreferenzseiten

Jede Richtlinienreferenzseite enthält die folgenden Informationen:

- Verwenden dieser Richtlinie – Ob Sie die Richtlinie an Benutzer, Gruppen und Rollen anfügen können
- Richtliniendetails
  - Typ – Der Typ der AWS verwalteten Richtlinie
    - `AWS managed policy` – Eine AWS verwaltete Standardrichtlinie
    - `Job function policy` – Richtlinie, die auf gängige Job-Funktionen in der Branche abgestimmt ist
    - `Service-linked role policy` – Richtlinie, die einer serviceverknüpften Rolle zugeordnet ist, die es einem Service ermöglicht, Aktionen in Ihrem Namen auszuführen, z. B. the section called “AmazonRDSPreviewServiceRolePolicy”

    - `Service role policy` – Richtlinie, die für die Arbeit mit Servicerollen entwickelt wurde, z. B. the section called “AWSControlTowerServiceRolePolicy”
  - Erstellungszeit – wann die Richtlinie zum ersten Mal erstellt wurde
  - Bearbeitungszeit – Wann diese Version der Richtlinie bearbeitet wurde
  - ARN – Der Amazon-Ressourcenname der Richtlinie
- Richtlinienversion – Die Version der Berechtigungen, die von der Richtlinie gewährt werden
- JSON-Richtliniendokument – Die JSON-Richtlinie
- Weitere Informationen – Links zur Dokumentation im Zusammenhang mit von AWS verwalteten Richtlinien

Veraltete, von AWS verwaltete Richtlinien

AWS aktualisiert regelmäßig AWS verwaltete Richtlinien. In den meisten Fällen fügen wir einer Richtlinie Berechtigungen hinzu. Dies geschieht, wenn wir einen neuen Service oder eine neue Funktion starten. Um die Sicherheit AWS verwalteter Richtlinien zu verbessern, reduzieren wir manchmal den Geltungsbereich von Richtlinien. Wenn wir Berechtigungen aus einer Richtlinie entfernen, setzen wir die Richtlinie auf einen veralteten Status und machen einen neuen verfügbar. Wenn einen Service oder ein Feature AWS als veraltet einstuft, wird auch die AWS von verwaltete Richtlinie für dieses Feature als veraltet eingestuft.

Wenn Sie eine E-Mail-Benachrichtigung erhalten, dass eine von Ihnen verwendete Richtlinie veraltet ist, empfehlen wir Ihnen, sofort Maßnahmen zu ergreifen. Identifizieren Sie die Änderung der Richtlinie und aktualisieren Sie Ihre Workflows. Wenn eine Ersatzrichtlinie AWS bereitstellt, planen Sie, sie allen betroffenen Identitäten (Benutzer, Gruppen und Rollen) anzufügen und dann die veraltete Richtlinie von diesen Identitäten zu trennen.

Eine veraltete Richtlinie hat folgende Merkmale:

- Es wird aus diesem Handbuch entfernt.
- Berechtigungen funktionieren weiterhin für alle derzeit angefügten Identitäten.
- In Konten, in denen die Richtlinie an eine Identität angefügt ist, wird sie in der Liste Richtlinien in der IAM-Konsole mit einem Warnsymbol daneben angezeigt.
- Sie kann keinen neuen Identitäten zugeordnet werden. Wenn Sie sie von einer aktuellen Identität trennen, können Sie sie nicht erneut anfügen.
- Nachdem Sie es von allen aktuellen Entitäten getrennt haben, ist es nicht mehr sichtbar.

AWS Von verwaltete Richtlinien

AWS Von verwaltete Richtlinien

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- VPCLatticeReadOnlyAccess
- VPCLatticeServicesInvokeAccess
- WAFLoggingServiceRolePolicy
- WAFRegionalLoggingServiceRolePolicy
- WAFV2LoggingServiceRolePolicy
- WellArchitectedConsoleFullAccess
- WellArchitectedConsoleReadOnlyAccess
- WorkLinkServiceRolePolicy

AccessAnalyzerServiceRolePolicy

`AccessAnalyzerServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Access Analyzer die Analyse von Ressourcenmetadaten erlauben

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 02. Dezember 2019, 17:13 UTC
- Bearbeitungszeit: 22. Januar 2024, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AdministratorAccess

`AdministratorAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf - AWS Services und -Ressourcen.

Verwenden dieser Richtlinie

Sie können `AdministratorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. Februar 2015, 18:39 UTC
- Bearbeitungszeit: 06. Februar 2015, 18:39 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AdministratorAccess-Amplify

`AdministratorAccess-Amplify`ist eine AWSverwaltete Richtlinie, die: Konten Administratorberechtigungen gewährt und gleichzeitig ausdrücklich den direkten Zugriff auf Ressourcen ermöglicht, die von Amplify-Anwendungen benötigt werden.

Verwenden Sie diese -Richtlinie

Sie können Verbindungen `AdministratorAccess-Amplify` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2020, 19:03 UTC
- Bearbeitete Zeit: 31. Mai 2023, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

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

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

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

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

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

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

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

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte AWS mit den geringsten Berechtigungen

AdministratorAccess-AWSElasticBeanstalk

`AdministratorAccess-AWSElasticBeanstalk`ist eine AWSverwaltete Richtlinie, die: Dem Konto Administratorberechtigungen gewährt. Ermöglicht Entwicklern und Administratoren ausdrücklich den direkten Zugriff auf Ressourcen, die sie für die Verwaltung vonAWS Elastic Beanstalk Beanstalk-Anwendungen benötigen

Verwenden dieser -Richtlinie

Sie können`AdministratorAccess-AWSElasticBeanstalk` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. Januar 2021, 19:36 UTC
- Bearbeitete Zeit: 23. März 2023, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätset-Berechtigungen

- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AlexaForBusinessDeviceSetup

`AlexaForBusinessDeviceSetup`ist eine AWSverwaltete Richtlinie, die: Geräteeinstellungen Zugriff auf AlexaForBusiness Dienste gewährt

Verwenden dieser Richtlinie

Sie können`AlexaForBusinessDeviceSetup` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. November 2017, 16:47 UTC
- Bearbeitete Zeit: 20. Mai 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AlexaForBusinessFullAccess

`AlexaForBusinessFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf AlexaForBusiness Ressourcen und Zugriff auf verwandte Ressourcen gewährtAWS-Services

Verwenden dieser Richtlinie

Sie können`AlexaForBusinessFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. November 2017, 16:47 UTC
- Bearbeitete Zeit: 1. Juli 2020, 21:01 UTC

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

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AlexaForBusinessGatewayExecution

`AlexaForBusinessGatewayExecution`ist eine AWSverwaltete Richtlinie, die: Gateway-Ausführungszugriff auf AlexaForBusiness Dienste bereitstellt

Verwenden dieser -Richtlinie

Sie können`AlexaForBusinessGatewayExecution` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. November 2017, 16:47 UTC
- Bearbeitete Zeit: 30. November 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und verwaltete Richtlinien

AlexaForBusinessLifesizeDelegatedAccessPolicy

`AlexaForBusinessLifesizeDelegatedAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Lifesize AVS-Geräte ermöglicht

Verwenden dieser Richtlinie

Sie können`AlexaForBusinessLifesizeDelegatedAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. Juni 2020, 19:46 UTC

- Bearbeitete Zeit: 12. Juni 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete Standardversion ist die -verwaltete Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AlexaForBusinessNetworkProfileServicePolicy

`AlexaForBusinessNetworkProfileServicePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es Alexa for Business, automatisierte Aufgaben auszuführen, die nach Ihren Netzwerkprofilen geplant sind.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 13. März 2019, 00:53 UTC
- Bearbeitete Zeit: 5. April 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinien für die Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONRichtelement

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AlexaForBusinessPolyDelegatedAccessPolicy

`AlexaForBusinessPolyDelegatedAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Poly AVS-Geräte gewährt

Verwenden dieser Richtlinie

Sie können`AlexaForBusinessPolyDelegatedAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 16. Oktober 2019, 19:48 UTC
- Bearbeitete Zeit: 16. Oktober 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Dokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AlexaForBusinessReadOnlyAccess

`AlexaForBusinessReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf AlexaForBusiness Dienste gewährt

Verwenden dieser -Richtlinie

Sie können`AlexaForBusinessReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. November 2017, 16:47 UTC
- Bearbeitete Zeit: 20. November 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete Richtlinie ist die -verwaltete -verwaltete Version der -verwaltete Richtlinien. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAPIGatewayAdministrator

`AmazonAPIGatewayAdministrator`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf das Erstellen/Bearbeiten/Löschen von APIs in Amazon API Gateway über die bietetAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AmazonAPIGatewayAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Juli 2015, 17:34 UTC
- Bearbeitete Zeit: 9. Juli 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie ist die -verwaltete Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAPIGatewayInvokeFullAccess

`AmazonAPIGatewayInvokeFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf das Aufrufen von APIs in Amazon API Gateway bietet.

Verwenden dieser -Richtlinie

Sie könnenAmazonAPIGatewayInvokeFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Juli 2015, 17:36 UTC
- Bearbeitete Zeit: 18. Dezember 2018, 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAPIGatewayPushToCloudWatchLogs

`AmazonAPIGatewayPushToCloudWatchLogs`ist eine AWSverwaltete Richtlinie, die: Es API Gateway ermöglicht, Protokolle an das Benutzerkonto zu übertragen.

Verwenden dieser -Richtlinie

Sie können`AmazonAPIGatewayPushToCloudWatchLogs` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 11. November 2015, 23:41 UTC
- Bearbeitete Zeit: 11. November 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAppFlowFullAccess

`AmazonAppFlowFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon AppFlow und Zugriff aufAWS Dienste bietet, die als Flow-Quelle oder Ziel unterstützt werden (S3 und Redshift). Bietet auch Zugriff auf KMS zur Verschlüsselung

Verwenden dieser -Richtlinie

Sie können`AmazonAppFlowFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. Juni 2020, 23:30 UTC
- Bearbeitete Zeit: 28. Februar 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAppFlowReadOnlyAccess

`AmazonAppFlowReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Appflow-Flows bietet

Verwenden dieser -Richtlinie

Sie können`AmazonAppFlowReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. Juni 2020, 23:26 UTC
- Bearbeitete Zeit: 28. Februar 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAppStreamFullAccess

`AmazonAppStreamFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon AppStream über die bietetAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AmazonAppStreamFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 28. August 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die Standardversion der -Richtlinie ist die -verwaltete Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAppStreamPCAAccess

`AmazonAppStreamPCAAccess`ist eine AWSverwaltete Richtlinie, die: Amazon AppStream 2.0-Zugriff aufAWS Certificate Manager Private CA in Kundenkonten zur zertifikatsbasierten Authentifizierung

Verwenden dieser -Richtlinie

Sie können`AmazonAppStreamPCAAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 24. Oktober 2022, 17:05 UTC
- Bearbeitete Zeit: 24. Oktober 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAppStreamReadOnlyAccess

`AmazonAppStreamReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht Lesezugriff auf Amazon AppStream über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonAppStreamReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 7. Dezember 2016, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON--Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAppStreamServiceAccess

`AmazonAppStreamServiceAccess`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die AppStream Amazon-Servicerolle.

Verwenden dieser Richtlinien

Sie können`AmazonAppStreamServiceAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 19. November 2016, 04:17 UTC
- Bearbeitete Zeit: 26. Juni 2020, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAthenaFullAccess

`AmazonAthenaFullAccess` ist eine -AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Athena und eingeschränkten Zugriff auf die Abhängigkeiten bietet, die für das Abfragen, Schreiben von Ergebnissen und Datenmanagement erforderlich sind.

Verwenden dieser Richtlinie

Sie können `AmazonAthenaFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 16:46 UTC
- Bearbeitungszeit: 03. Januar 2024, 19:05 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Richtlinienversion

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonAugmentedAIFullAccess

`AmazonAugmentedAIFullAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Ausführung aller Amazon Augmented AI-Ressourcen bietet FlowDefinitions, einschließlich HumanTaskUis und HumanLoops. Erlaubt keinen Zugriff, um FlowDefinitions gegen das öffentliche Workteam zu arbeiten.

Verwenden dieser Richtlinie

Sie können`AmazonAugmentedAIFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 16:21 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAugmentedAIHumanLoopFullAccess

`AmazonAugmentedAIHumanLoopFullAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Ausführung aller Operationen bietet HumanLoops.

Verwenden dieser Richtlinie

Sie können`AmazonAugmentedAIHumanLoopFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 3. Dezember 2019, 16:20 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonAugmentedAIIntegratedAPIAccess

`AmazonAugmentedAIIntegratedAPIAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf alle Vorgänge gewährt, die Amazon Augmented AI-Ressourcen ausführen können FlowDefinitions, einschließlich HumanTaskUis und HumanLoops. Bietet auch Zugriff auf die Abläufe von Diensten, die in Amazon Augmented AI integriert sind.

Verwenden dieser Richtlinien

Sie können`AmazonAugmentedAIIntegratedAPIAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. April 2020, 20:47 UTC
- Bearbeitete Zeit: 22. April 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AmazonBedrockFullAccess

`AmazonBedrockFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Bedrock sowie eingeschränkten Zugriff auf zugehörige Dienste bietet, die für Amazon Bedrock erforderlich sind

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonBedrockFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2023, 15:47 UTC
- Bearbeitete Zeit: 6. Dezember 2023, 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockReadOnly

`AmazonBedrockReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf Amazon Bedrock gewährt

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonBedrockReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2023, 15:48 UTC
- Bearbeitete Zeit: 6. Dezember 2023, 15:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBraketFullAccess

`AmazonBraketFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Braket über dasAWS Management Console und SDK bietet. Bietet auch Zugriff auf verwandte Dienste (z. B. S3, Logs).

Verwenden dieser -Richtlinie

Sie können`AmazonBraketFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. August 2020, 20:12 UTC
- Bearbeitete Zeit: 19. April 2023, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonBraketJobsExecutionPolicy

`AmazonBraketJobsExecutionPolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff aufAWS-Services und Ressourcen gewährt, die für die Ausführung eines Amazon Braket-Jobs erforderlich sind, einschließlich S3, Cloudwatch, IAM und Braket

Verwenden dieser -Richtlinie

Sie können`AmazonBraketJobsExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. November 2021, 19:34 UTC
- Bearbeitete Zeit: 28. November 2021, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonBraketServiceRolePolicy

`AmazonBraketServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Braket ermöglicht,AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 4. August 2020, 17:12 UTC
- Bearbeitete Zeit: 6. August 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standarddokument Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AmazonChimeFullAccess

`AmazonChimeFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die Amazon Chime Admin Console über die bietetAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonChimeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. November 2017, 22:15 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonChimeReadOnly

`AmazonChimeReadOnly`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf die Amazon Chime Admin Console über dieAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AmazonChimeReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. November 2017, 22:04 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Version der Richtlinie

Version der Richtlinie:v10 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen mit den geringsten Berechtigungen Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen geringsten Berechtigungen Berechtigungen geringsten Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen

AmazonChimeSDK

`AmazonChimeSDK`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Amazon Chime SDK-Operationen gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonChimeSDK` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. Februar 2020, 21:53 UTC
- Bearbeitete Zeit: 10. Januar 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -verwaltete -verwaltete -Richtlinie definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Verwaltete Richtlinie für Amazon Chime SDK MediaPipelines Service Linked Role

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. April 2022, 22:02 UTC
- Bearbeitete Zeit: 8. Dezember 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeSDKMessagingServiceRolePolicy

`AmazonChimeSDKMessagingServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Chime SDK Messaging den Zugriff aufAWS Ressourcen und die Aktivierung der Messaging-Funktionalität ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 3. März 2023, 01:43 UTC
- Bearbeitete Zeit: 3. März 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienelement

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AmazonChimeServiceRolePolicy

`AmazonChimeServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS Ressourcen ermöglicht, die von Amazon Chime verwendet oder verwaltet werden

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 30. September 2019, 22:25 UTC
- Bearbeitete Zeit: 30. September 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Richtlinie ist die Richtlinie zugeordnet. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AmazonChimeTranscriptionServiceLinkedRolePolicy

`AmazonChimeTranscriptionServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Chime den Zugriff auf Amazon Transcribe und Amazon Transcribe Medical in Ihrem Namen ermöglicht

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die servicegebundene Rolle in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 4. August 2021, 21:47 UTC
- Bearbeitete Zeit: 4. August 2021, 21:47 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Berechtigungen für die Richtlinie definiert. Die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtelement

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS den geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen und Berechtigungen

AmazonChimeUserManagement

`AmazonChimeUserManagement`ist eine AWSverwaltete Richtlinie, die: Ermöglicht Benutzerverwaltungszugriff auf die Amazon Chime Admin Console über dieAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonChimeUserManagement` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. November 2017, 22:17 UTC
- Bearbeitete Zeit: 18. Februar 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Verwaltete Richtlinie für Service Linked Role für Amazon Chime VoiceConnector

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 30. September 2019, 22:16 UTC
- Bearbeitete Zeit: 14. April 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCloudDirectoryFullAccess

`AmazonCloudDirectoryFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Cloud Directory Service bietet.

Verwenden dieser Richtlinie

Sie können`AmazonCloudDirectoryFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. Februar 2017, 00:41 UTC
- Bearbeitete Zeit: 25. Februar 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCloudDirectoryReadOnlyAccess

`AmazonCloudDirectoryReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Cloud Directory Service gewährt.

Verwenden dieser -Richtlinie mit diesen Richtlinien

Sie können`AmazonCloudDirectoryReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2017, 23:42 UTC
- Bearbeitete Zeit: 28. Februar 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
        "clouddirectory:List*",
        "clouddirectory:Get*",
        "clouddirectory:LookupPolicy",
        "clouddirectory:BatchRead"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen und -verwalteter Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCloudWatchEvidentlyFullAccess

`AmazonCloudWatchEvidentlyFullAccess`ist eine AWSverwaltete Richtlinie, die: CloudWatch Evidently vollen Zugriff nur auf Amazon gewährt. Bietet auch Zugriff auf verwandte Amazon S3, Amazon SNS CloudWatch, Amazon und andere verwandte Dienste.

Verwenden dieser -Richtlinie

Sie können`AmazonCloudWatchEvidentlyFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2021, 15:10 UTC
- Bearbeitete Zeit: 29. November 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCloudWatchEvidentlyReadOnlyAccess

`AmazonCloudWatchEvidentlyReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: CloudWatch Offensichtlich Lesezugriff auf Amazon gewährt

Verwenden dieser Richtlinie

Sie könnenAmazonCloudWatchEvidentlyReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2021, 15:08 UTC
- Bearbeitete Zeit: 29. November 2021, 15:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCloudWatchEvidentlyServiceRolePolicy

`AmazonCloudWatchEvidentlyServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es CloudWatch Evidently Service ermöglicht, die zugehörigenAWS Ressourcen im Namen des Kunden zu verwalten

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 13. September 2022, 17:25 UTC
- Bearbeitete Zeit: 13. September 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCloudWatchRUMFullAccess

`AmazonCloudWatchRUMFullAccess`ist eine AWSverwaltete Richtlinie, die: volle Zugriffsberechtigungen für den Amazon CloudWatch RUM-Dienst gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonCloudWatchRUMFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 29. November 2021, 15:46 UTC
- Bearbeitete Zeit: 29. November 2021, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AmazonCloudWatchRUMReadOnlyAccess

`AmazonCloudWatchRUMReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Leserechte für den Amazon CloudWatch RUM-Dienst gewährt

Verwenden

Sie können`AmazonCloudWatchRUMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2021, 15:43 UTC
- Bearbeitete Zeit: 28. Oktober 2022, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen
- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS und Umstellung auf die geringsten Berechtigungen

AmazonCloudWatchRUMServiceRolePolicy

`AmazonCloudWatchRUMServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon CloudWatch RUM Service die Erlaubnis erteilt, Überwachungsdaten für andere relevanteAWS Dienste zu veröffentlichen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. November 2021, 23:17 UTC
- Bearbeitete Zeit: 22. Februar 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCodeCatalystFullAccess

`AmazonCodeCatalystFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon bietetCodeCatalyst

Verwenden von dieser Richtlinie von -Richtlinie

Sie können`AmazonCodeCatalystFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. April 2023, 16:50 UTC
- Bearbeitete Zeit: 20. April 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinie von JSON

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

```
    {
      "Sid" : "CodeCatalystAssociateIAMRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codecatalyst.amazonaws.com",
            "codecatalyst-runner.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von IAM-Richtlinie IAM-Richtlinie IAM-Richtlinie für IAM-Richtlinie
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinie mit den geringsten verwaltete Richtlinie mit den geringsten verwaltete Richtlinie mit den geringsten verwaltete

AmazonCodeCatalystReadOnlyAccess

`AmazonCodeCatalystReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon gewährt CodeCatalyst

Verwenden dieser Richtlinie

Sie können`AmazonCodeCatalystReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 20. April 2023, 16:49 UTC
- Bearbeitete Zeit: 20. April 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCodeCatalystSupportAccess

`AmazonCodeCatalystSupportAccess`ist eine AWSverwaltete Richtlinie, die: Amazon ermöglicht,AWS Support Fälle in Ihrem Namen CodeCatalyst zu erstellen, zu aktualisieren und zu lösen.

Verwenden dieser Richtlinien

Sie können`AmazonCodeCatalystSupportAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 20. April 2023, 12:34 UTC
- Bearbeitete Zeit: 20. April 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCodeGuruProfilerAgentAccess

`AmazonCodeGuruProfilerAgentAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht den Zugriff, den der Amazon CodeGuru Profiler-Agent benötigt.

Verwenden dieser Richtlinien

Sie können`AmazonCodeGuruProfilerAgentAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 5. Februar 2021, 22:11 UTC
- Bearbeitete Zeit: 5. Mai 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinien ist die -Richtlinie, die die Berechtigungen für die -Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCodeGuruProfilerFullAccess

`AmazonCodeGuruProfilerFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon CodeGuru Profiler bietet.

Verwenden dieser Richtlinie

Sie können`AmazonCodeGuruProfilerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 10:13 UTC
- Bearbeitete Zeit: 15. Juli 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCodeGuruProfilerReadOnlyAccess

`AmazonCodeGuruProfilerReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon CodeGuru Profiler gewährt.

Verwenden dieser Richtlinien

Sie können`AmazonCodeGuruProfilerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 3. Dezember 2019, 10:30 UTC
- Bearbeitete Zeit: 27. Juni 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie ist die Version, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf mit den geringsten Richtlinien

AmazonCodeGuruReviewerFullAccess

`AmazonCodeGuruReviewerFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon CodeGuru Reviewer und eingeschränkten Zugriff auf die erforderlichen Abhängigkeiten gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonCodeGuruReviewerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 08:33 UTC
- Bearbeitete Zeit: 29. August 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCodeGuruReviewerReadOnlyAccess

`AmazonCodeGuruReviewerReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Amazon CodeGuru Reviewer nur Lesezugriff gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonCodeGuruReviewerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 08:48 UTC
- Bearbeitete Zeit: 29. August 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCodeGuruReviewerServiceRolePolicy

`AmazonCodeGuruReviewerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Eine mit dem Service verknüpfte Rolle, die Amazon CodeGuru Reviewer benötigt, um in Ihrem Namen auf Ressourcen zuzugreifen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 3. Dezember 2019, 05:31 UTC
- Bearbeitete Zeit: 27. November 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCodeGuruSecurityFullAccess

`AmazonCodeGuruSecurityFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf AmazonCodeGuru Security bietet.

Verwenden dieser -Richtlinie

Sie könnenAmazonCodeGuruSecurityFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Mai 2023, 21:03 UTC
- Bearbeitete Zeit: 9. Mai 2023, 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie definiert die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen IAM-Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit denAWS verwaltete Richtlinien und Umstellung auf Berechtigungen

AmazonCodeGuruSecurityScanAccess

`AmazonCodeGuruSecurityScanAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht den Zugriff, der für die Arbeit mit AmazonCodeGuru Security-Scans erforderlich ist.

Verwenden von dieser -Richtlinie

Sie können`AmazonCodeGuruSecurityScanAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Mai 2023, 20:54 UTC
- Bearbeitete Zeit: 9. Mai 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinie

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinie
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinie und und und und und und mit -verwaltete Richtlinie und und und und und mit -verwaltete

AmazonCognitoDeveloperAuthenticatedIdentities

`AmazonCognitoDeveloperAuthenticatedIdentities`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Amazon Cognito Cognito-APIs bietet, um von Entwicklern authentifizierte Identitäten von Ihrem Authentifizierungs-Backend aus zu unterstützen.

Verwenden dieser -Richtlinie

Sie können`AmazonCognitoDeveloperAuthenticatedIdentities` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. März 2015, 17:22 UTC

- Bearbeitete Zeit: 24. März 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie ist die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCognitoIdpEmailServiceRolePolicy

`AmazonCognitoIdpEmailServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Ermöglicht dem Amazon Cognito User Pools Service, Ihre SES-Identitäten für den E-Mail-Versand zu verwenden

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. März 2019, 21:32 UTC
- Bearbeitete Zeit: 21. März 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCognitoIdpServiceRolePolicy

`AmazonCognitoIdpServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und Ressourcen, die von Amazon Cognito Cognito-Benutzerpools verwendet oder verwaltet werden, ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. Juni 2020, 22:30 UTC
- Bearbeitete Zeit: 26. Juni 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCognitoPowerUser

`AmazonCognitoPowerUser`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff auf bestehende Amazon Cognito Cognito-Ressourcen bietet. Sie benötigenAWS-Konto Administratorrechte, um neue Cognito-Ressourcen zu erstellen.

Verwenden dieser -Richtlinie

Sie können`AmazonCognitoPowerUser` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. März 2015, 17:14 UTC
- Bearbeitete Zeit: 1. Juni 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und -verwaltete Richtlinien und -verwaltete Richtlinien

AmazonCognitoReadOnly

`AmazonCognitoReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Cognito Cognito-Ressourcen gewährt.

Verwenden dieser Richtlinie

Sie können`AmazonCognitoReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. März 2015, 17:06 UTC
- Bearbeitete Zeit: 1. August 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonCognitoUnAuthedIdentitiesSessionPolicy

`AmazonCognitoUnAuthedIdentitiesSessionPolicy`ist einAWSverwaltete Richtliniedas: Diese Richtlinie definiert den Satz von Berechtigungen, die für nicht authentifizierte Identitäten für Cognito Identity Pools zulässig sind. Diese Richtlinie soll nicht als eigenständige Genehmigungsrichtlinie verwendet werden. Es dient als Schutzmaßnahme gegen übermäßig freizügige Richtlinien, die für Rollen in einem Identitätspool gelten. Ordnen Sie diese Richtlinie keiner Rolle zu, da Cognito Identity Service sie bei der Erstellung von Anmeldeinformationen automatisch als Richtlinie mit begrenztem Geltungsbereich einbezieht. Die Rechte, vorübergehend auf andere zuzugreifenAWSDie Ressourcen, die durch den erweiterten Datenfluss bereitgestellt werden, werden nun durch den Schnittpunkt zwischen der Rolle, die mit der Identität des nicht authentifizierten Benutzers verknüpft ist, die von einem Dienst bereitgestellt wird, und den Rechten definiert, die in dieser verwalteten Richtlinie gewährt werden, die Cognito gehört.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonCognitoUnAuthedIdentitiesSessionPolicy`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 19. Juli 2023, 23:04 Uhr UTC
- Uhrzeit der Bearbeitung:19. Juli 2023, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonCognitoUnauthenticatedIdentities

`AmazonCognitoUnauthenticatedIdentities`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie definiert den Satz von Berechtigungen, die für nicht authentifizierte Identitäten für Cognito-Identitätspools zulässig sind. Dies muss nicht an Ihre Unauth-Rolle angehängt werden, da Cognito Identity Service es bei der Erstellung von Anmeldeinformationen automatisch als Richtlinie mit begrenztem Gültigkeitsbereich einbezieht. Die Rechte für den temporären Zugriff auf andereAWS Ressourcen über den erweiterten Ablauf werden nun anhand der Schnittstelle zwischen der Rolle definiert, die der Identität des nicht authentifizierten Benutzers zugeordnet ist, die von einem Dienst bereitgestellt wird, und den Rechten, die in dieser verwalteten Richtlinie gewährt werden, die Eigentum von Cognito ist.

Verwenden dieser -Richtlinie

Sie können`AmazonCognitoUnauthenticatedIdentities` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Februar 2023, 22:36 UTC
- Bearbeitete Zeit: 1. Februar 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardrichtlinie ist die -Standardversion, die die Berechtigungen für die -Standardrichtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt, wird die Standardversion der RichtlinieAWS überprüft, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonConnect_FullAccess

`AmazonConnect_FullAccess`ist eine AWSverwaltete Richtlinie, die: Der Zweck dieser Richtlinie besteht darin,AWS Connect-Benutzern Berechtigungen zu gewähren, die für die Nutzung von Connect-Ressourcen erforderlich sind. Diese Richtlinie bietet vollständigen Zugriff aufAWS Connect-Ressourcen über die Connect Console und öffentliche APIs über die Connect Console und die öffentlichen APIs.

Verwenden dieser Richtlinie verwenden dieser Richtlinie

Sie können`AmazonConnect_FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. November 2020, 19:54 UTC
- Bearbeitete Zeit: 7. März 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der -Richtlinie ist die -Standardversion der -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den

AmazonConnectCampaignsServiceLinkedRolePolicy

`AmazonConnectCampaignsServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie für mit dem Service Amazon Connect Campaigns verknüpfte Rolle

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. September 2021, 20:54 UTC
- Bearbeitete Zeit: 8. November 2023, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectReadOnlyAccess

`AmazonConnectReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Erteilt die Erlaubnis, die Amazon Connect Connect-Instances in IhremAWS-Konto.

Verwenden dieser -Richtlinie

Sie können`AmazonConnectReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. Oktober 2018, 21:00 UTC
- Bearbeitete Zeit: 6. November 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie ist die für die -Richtlinie definiert, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete mit -verwaltete mit -verwaltete mit -verwaltete

AmazonConnectServiceLinkedRolePolicy

`AmazonConnectServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Connect ermöglicht, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

Diese Richtlinie verwenden

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. September 2018, 00:21 UTC
- Bearbeitete Zeit: 28. November 2023, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectSynchronizationServiceRolePolicy

`AmazonConnectSynchronizationServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Connect ermöglicht, AWS Ressourcen in Ihrem Namen regionsübergreifend zu synchronisieren.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. Oktober 2023, 22:38 UTC
- Bearbeitete Zeit: 27. Oktober 2023, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectVoiceIDFullAccess

`AmazonConnectVoiceIDFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Connect Voice ID gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonConnectVoiceIDFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. September 2021, 19:04 UTC
- Bearbeitete Zeit: 26. September 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDataZoneDomainExecutionRolePolicy

`AmazonDataZoneDomainExecutionRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Standardrichtlinie für die DomainExecutionRole Servicerolle DataZonevon Amazon . Diese Rolle wird von Amazon verwendet, DataZone um Daten in der Amazon- DataZone Domain zu katalogisieren, zu entdecken, zu verwalten, freizugeben und zu analysieren.

Verwenden dieser Richtlinie

Sie können `AmazonDataZoneDomainExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 27. September 2023, 21:55 UTC
- Bearbeitungszeit: 12. März 2024, 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Richtlinienversion

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

```
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
```

```
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetListing",
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListNotifications",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:UpdateDataSource",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
```

```
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonDataZoneEnvironmentRolePermissionsBoundary

`AmazonDataZoneEnvironmentRolePermissionsBoundary`ist eine AWSverwaltete Richtlinie, die: Amazon DataZone erstellt IAM-Rollen für Umgebungen, um Datenanalyseaktionen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenze ihrer Berechtigungen zu definieren.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneEnvironmentRolePermissionsBoundary` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. September 2023, 23:38 UTC
- Bearbeitete Zeit: 17. November 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneFullAccess

`AmazonDataZoneFullAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf Amazon DataZone über die AWS Management Console sowie eingeschränkten Zugriff auf zugehörige -Services, die von ihr benötigt werden.

Verwenden dieser Richtlinie

Sie können `AmazonDataZoneFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 20:06 UTC
- Bearbeitungszeit: 12. März 2024, 16:34 UTC

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

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

```
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : "s3:CreateBucket",
      "Resource" : "arn:aws:s3:::amazon-datazone*"
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
```

```
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*",
```

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonDataZoneFullUserAccess

`AmazonDataZoneFullUserAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf Amazon DataZone, aber nicht die Verwaltung von Domains, Benutzern oder zugehörigen Konten erlaubt.

Verwenden dieser Richtlinie

Sie können `AmazonDataZoneFullUserAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 21:06 UTC
- Bearbeitungszeit: 12. März 2024, 23:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Richtlinienversion

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
```

```
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
```

```
        "datazone:DeleteProjectMembership",
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonDataZoneGlueManageAccessRolePolicy

`AmazonDataZoneGlueManageAccessRolePolicy`ist eine AWSverwaltete Richtlinie, die: Die Richtlinie gewährt Amazon Berechtigungen, DataZone um die Veröffentlichung und den Zugriff auf Daten zu ermöglichen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneGlueManageAccessRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. September 2023, 20:21 UTC
- Bearbeitete Zeit: 14. Dezember 2023, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZonePortalFullAccessPolicy

`AmazonDataZonePortalFullAccessPolicy`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf DataZone Amazon-APIs bietet

Verwenden dieser -Richtlinie

Sie können`AmazonDataZonePortalFullAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. März 2023, 18:24 UTC
- Bearbeitete Zeit: 26. März 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDataZonePreviewConsoleFullAccess

`AmazonDataZonePreviewConsoleFullAccess`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff auf die Vorschauversion von AmazonDataZoneüber dieAWS Management Console. Bietet auch ausgewählten Zugriff auf andere verwandte Dienste.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonDataZonePreviewConsoleFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 28. März 2023, 15:16 Uhr UTC
- Uhrzeit der Bearbeitung:13. Juli 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie: v2(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonDataZoneProjectDeploymentPermissionsBoundary

`AmazonDataZoneProjectDeploymentPermissionsBoundary`ist eine AWSverwaltete Richtlinie, die: Amazon DataZone erstellt IAM-Rollen, die es für die Bereitstellung von Datenanalyseprojekten verwendet. DataZone verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

Verwenden dieser -Richtlinie

Sie können`AmazonDataZoneProjectDeploymentPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. März 2023, 02:54 UTC
- Bearbeitete Zeit: 4. April 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDataZoneProjectRolePermissionsBoundary

`AmazonDataZoneProjectRolePermissionsBoundary`ist eine AWSverwaltete Richtlinie, die: Amazon DataZone erstellt IAM-Rollen für Projekte zur Durchführung von Datenanalyseaktionen und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

Verwenden dieser -Richtlinie

Sie können`AmazonDataZoneProjectRolePermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. März 2023, 02:51 UTC
- Bearbeitete Zeit: 21. März 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDataZoneRedshiftGlueProvisioningPolicy

`AmazonDataZoneRedshiftGlueProvisioningPolicy` ist eine von AWS verwaltete Richtlinie, die: Amazon DataZone ist ein Datenverwaltungsservice, mit dem Sie Ihre Daten katalogisieren, entdecken, verwalten, freigeben und analysieren können. Mit Amazon können DataZoneSie Ihre Daten über Konten und unterstützte Regionen hinweg freigeben und darauf zugreifen. Amazon DataZone vereinfacht Ihre Erfahrung mit allen - AWS Services, einschließlich, aber nicht beschränkt auf Amazon Redshift, Amazon Athena , AWS Glue und AWS Lake Formation.

Verwenden dieser Richtlinie

Sie können `AmazonDataZoneRedshiftGlueProvisioningPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 20:19 UTC
- Bearbeitungszeit: 12. März 2024, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonDataZoneRedshiftManageAccessRolePolicy

`AmazonDataZoneRedshiftManageAccessRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie erteilt Amazon die DataZone Erlaubnis, Amazon Redshift Redshift-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf veröffentlichte Amazon Redshift- oder Amazon Redshift Serverless-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonDataZoneRedshiftManageAccessRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. September 2023, 20:15 UTC
- Bearbeitete Zeit: 16. November 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveFullAccess

`AmazonDetectiveFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den Amazon Detective-Dienst und eingeschränkten Zugriff auf die Abhängigkeiten der Konsolenbenutzeroberfläche bietet

Verwenden Sie diese -Richtlinie

Sie können`AmazonDetectiveFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Erstellungszeit: 30. April 2020, 17:57 UTC
- Bearbeitete Zeit: 17. Mai 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinie

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinie
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AmazonDetectiveInvestigatorAccess

`AmazonDetectiveInvestigatorAccess`ist eine AWSverwaltete Richtlinie, die: Ermittlern Zugriff auf den Amazon Detective Service und bereichsbezogenen Zugriff auf die Benutzeroberflächenabhängigkeiten der Konsole gewährt. Diese Richtlinie gewährt die Erlaubnis,

Detective zu Ermittlungszwecken zu nutzen, und gewährt eingeschränkten Schreibzugriff auf Guardduty.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonDetectiveInvestigatorAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Januar 2023, 15:24 UTC
- Bearbeitete Zeit: 27. November 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveMemberAccess

`AmazonDetectiveMemberAccess`ist eine AWSverwaltete Richtlinie, die: Mitgliedern Zugriff auf den Amazon Detective-Dienst und eingeschränkten Zugriff auf die Abhängigkeiten der Konsolenbenutzeroberfläche bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonDetectiveMemberAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. Januar 2023, 15:16 UTC
- Bearbeitete Zeit: 17. Januar 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete Version definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Berechtigungen

AmazonDetectiveOrganizationsAccess

`AmazonDetectiveOrganizationsAccess`ist eine AWSverwaltete Richtlinie, die: Organizations Zugriff auf die Verwaltung des delegierten Administrators für Amazon Detective und eingeschränkten Zugriff auf die Abhängigkeiten der Konsolenbenutzeroberfläche bietet. Dies erteilt auch die Berechtigung zum Erstellen einer serviceverknüpften Rolle für Detective.

Verwenden dieser -Richtlinie

Sie könnenAmazonDetectiveOrganizationsAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. März 2023, 15:20 UTC
- Bearbeitete Zeit: 2. März 2023, 15:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDetectiveServiceLinkedRolePolicy

`AmazonDetectiveServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Detective ermöglicht, in Ihrem Namen Serviceanrufe zu tätigen

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. November 2021, 19:47 UTC
- Bearbeitete Zeit: 18. November 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardelement ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtdokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Die Richtlinie gewährt vollen Zugriff auf die DevOps Guru-Konsole.

Verwenden dieser Richtlinien

Sie können`AmazonDevOpsGuruConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 17. Dezember 2021, 18:43 UTC
- Bearbeitete Zeit: 25. August 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon DevOps Guru bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonDevOpsGuruFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2020, 16:38 UTC
- Bearbeitete Zeit: 25. August 2022, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und -verwaltete Richtlinien

AmazonDevOpsGuruOrganizationsAccess

`AmazonDevOpsGuruOrganizationsAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff gewährt, um Amazon DevOps Guru innerhalb einer Organisation zu aktivieren und zu verwalten.

Verwenden dieser -Richtlinie

Sie können`AmazonDevOpsGuruOrganizationsAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. November 2021, 23:50 UTC
- Bearbeitete Zeit: 15. November 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDevOpsGuruReadOnlyAccess

`AmazonDevOpsGuruReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf die Amazon DevOps Guru Console gewährt.

Verwenden dieser Richtlinie

Sie können`AmazonDevOpsGuruReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2020, 16:34 UTC
- Bearbeitete Zeit: 25. August 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDevOpsGuruServiceRolePolicy

`AmazonDevOpsGuruServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Eine servicegebundene Rolle, die Amazon für DevOpsGuru den Zugriff auf Ihre Ressourcen benötigt.

Verwenden Verwenden Verwenden Verwenden Verwenden Verwenden Verwenden Verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 1. Dezember 2020, 10:24 UTC
- Bearbeitete Zeit: 10. Januar 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v9 (Standard)

Die Standard-Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richt

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDMSCloudWatchLogsRole

`AmazonDMSCloudWatchLogsRole`ist eine AWSverwaltete Richtlinie, die: Zugriff auf das Hochladen von DMS-Replikationsprotokollen in Cloudwatch-Logs im Kundenkonto bietet.

Verwenden dieser -Richtlinie

Sie können Verbindungen `AmazonDMSCloudWatchLogsRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Diensträgerrollen
- Aufnahmezeit: 7. Januar 2016, 23:44 UTC
- Bearbeitete Zeit: 23. Mai 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDMSRedshiftS3Role

`AmazonDMSRedshiftS3Role`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Verwaltung von S3-Einstellungen für Redshift-Endpoints für DMS bietet.

Verwenden dieser Richtlinie

Sie können`AmazonDMSRedshiftS3Role` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 20. April 2016, 17:05 UTC
- Bearbeitete Zeit: 8. Juli 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDMSVPCManagementRole

`AmazonDMSVPCManagementRole`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Verwaltung von VPC-Einstellungen fürAWS verwaltete Kundenkonfigurationen bietet

Verwenden dieser -Richtlinie

Sie können`AmazonDMSVPCManagementRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 18. November 2015, 16:33 UTC
- Bearbeitete Zeit: 23. Mai 2016, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDocDB-ElasticServiceRolePolicy

`AmazonDocDB-ElasticServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon DocumentDB-Elastic die Verwaltung vonAWS Ressourcen in Ihrem Namen ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 30. November 2022, 14:17 UTC
- Bearbeitete Zeit: 30. November 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AmazonDocDBConsoleFullAccess

`AmazonDocDBConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die Verwaltung von Amazon DocumentDB mit MongoDB-Kompatibilität mithilfe von bietetAWS Management Console. Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos, Berechtigungen zum Erstellen und Bearbeiten von Amazon EC2 EC2-Instances und VPC-Konfigurationen, Berechtigungen zum Anzeigen und Auflisten

von Schlüsseln auf Amazon KMS sowie vollen Zugriff auf Amazon RDS und Amazon Neptune gewährt.

Verwenden dieser -Richtlinie

Sie könnenAmazonDocDBConsoleFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Januar 2019, 20:37 UTC
- Bearbeitete Zeit: 30. November 2022, 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDocDBElasticFullAccess

`AmazonDocDBElasticFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon DocumentDB Elastic Clusters und andere erforderliche Berechtigungen für die zugehörigen Abhängigkeiten wie EC2, KMS und IAM bietet. SecretsManager CloudWatch

Verwendung dieser Richtlinie

Sie können Verbindungen `AmazonDocDBElasticFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 5. Juni 2023, 13:51 UTC
- Bearbeitete Zeit: 21. Juni 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AmazonDocDBElasticReadOnlyAccess

`AmazonDocDBElasticReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon DoCDB-Elastic und Metriken bietet. CloudWatch

Verwendung dieser Richtlinie

Sie können Verbindungen `AmazonDocDBElasticReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Juni 2023, 14:37 UTC
- Bearbeitete Zeit: 21. Juni 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AmazonDocDBFullAccess

`AmazonDocDBFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon DocumentDB mit MongoDB-Kompatibilität bietet. Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos sowie vollen Zugriff auf Amazon RDS und Amazon Neptune gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonDocDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Januar 2019, 20:21 UTC
- Bearbeitete Zeit: 9. Januar 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- ErsteAWS Schritte mit den geringsten Berechtigungen

AmazonDocDBReadOnlyAccess

`AmazonDocDBReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon DocumentDB mit MongoDB-Kompatibilität bietet. Beachten Sie, dass diese Richtlinie auch Zugriff auf Amazon RDS- und Amazon Neptune Neptune-Ressourcen gewährt.

Verwenden dieser Richtlinie

Sie können`AmazonDocDBReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Januar 2019, 20:30 UTC
- Bearbeitete Zeit: 9. Januar 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDRSVPCManagement

`AmazonDRSVPCManagement`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Verwaltung von VPC-Einstellungen für von Amazon verwaltete Kundenkonfigurationen bietet

Verwenden dieser Richtlinie

Sie können`AmazonDRSVPCManagement` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. September 2015, 00:09 UTC
- Bearbeitete Zeit: 2. September 2015, 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion der -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDynamoDBFullAccess

`AmazonDynamoDBFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon DynamoDB über die bietetAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonDynamoDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 29. Januar 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Version der Richtlinie

Version der Richtlinie:v15 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDynamoDBFullAccesswithDataPipeline

`AmazonDynamoDBFullAccesswithDataPipeline`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist veraltet. Eine Anleitung finden Sie in der Dokumentation: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html. Bietet vollen Zugriff auf Amazon DynamoDB, einschließlich Export/Import mithilfe vonAWS Data Pipeline über dieAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonDynamoDBFullAccesswithDataPipeline` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 12. November 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonDynamoDBReadOnlyAccess

`AmazonDynamoDBReadOnlyAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf Amazon DynamoDB über die AWS Management Console.

Verwenden dieser Richtlinie

Sie können `AmazonDynamoDBReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. Februar 2015, 18:40 UTC
- Bearbeitungszeit: 20. März 2024, 15:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonEBSCSIDriverPolicy

`AmazonEBSCSIDriverPolicy`ist eine AWS-verwaltete -Richtlinie, mit welcher das Service-Konto in Ihrem Namen Aufrufe an -verwaltete Dienste wie EC2 tätigen kann.

Verwenden dieser Richtlinie

Sie können`AmazonEBSCSIDriverPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 4. April 2022, 17:24 UTC
- Bearbeitete Zeit: 18. November 2022, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der -Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2ContainerRegistryFullAccess

`AmazonEC2ContainerRegistryFullAccess`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff auf Amazon ECR-Ressourcen bietet

Verwenden dieser -Richtlinie

Sie können`AmazonEC2ContainerRegistryFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. Dezember 2015, 17:06 UTC
- Bearbeitete Zeit: 5. Dezember 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2ContainerRegistryPowerUser

`AmazonEC2ContainerRegistryPowerUser`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon EC2 Container Registry-Repositorys bietet, das Löschen von Repositorys oder Richtlinienänderungen jedoch nicht zulässt.

Verwenden dieser -Richtlinie

Sie können`AmazonEC2ContainerRegistryPowerUser` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. Dezember 2015, 17:05 UTC
- Bearbeitete Zeit: 10. Dezember 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2ContainerRegistryReadOnly

`AmazonEC2ContainerRegistryReadOnly`ist eine AWSverwaltete Richtlinie, die: Schreibgeschützten Zugriff auf Amazon EC2 Container Registry-Repositorys bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonEC2ContainerRegistryReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. Dezember 2015, 17:04 UTC
- Bearbeitete Zeit: 10. Dezember 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2ContainerServiceAutoscaleRole

`AmazonEC2ContainerServiceAutoscaleRole`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung von Task Autoscaling für Amazon EC2 Container Service

Verwenden dieser Richtlinie

Sie können`AmazonEC2ContainerServiceAutoscaleRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 12. Mai 2016, 23:25 UTC
- Bearbeitete Zeit: 5. Februar 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS

Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2ContainerServiceEventsRole

`AmazonEC2ContainerServiceEventsRole`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung von CloudWatch Events for EC2 Container Service

Verwenden dieser -Richtlinie

Sie können`AmazonEC2ContainerServiceEventsRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 30. Mai 2017, 16:51 UTC
- Bearbeitete Zeit: 6. März 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2ContainerServiceforEC2Role

`AmazonEC2ContainerServiceforEC2Role`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Amazon EC2-Rolle für Amazon EC2 Container Service.

Verwenden dieser -Richtlinie

Sie könnenAmazonEC2ContainerServiceforEC2Role an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 19. März 2015, 18:45 UTC
- Bearbeitete Zeit: 6. März 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2ContainerServiceRole

`AmazonEC2ContainerServiceRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Amazon ECS-Servicerolle.

Verwenden dieser -Richtlinie

Sie können`AmazonEC2ContainerServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 9. April 2015, 16:14 UTC
- Bearbeitete Zeit: 11. August 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2FullAccess

`AmazonEC2FullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon EC2 über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonEC2FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 27. November 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2ReadOnlyAccess

`AmazonEC2ReadOnlyAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf Amazon EC2 über die AWS Management Console.

Verwenden dieser Richtlinie

Sie können `AmazonEC2ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. Februar 2015, 18:40 UTC
- Bearbeitungszeit: 14. Februar 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforAWSCodeDeploy

`AmazonEC2RoleforAWSCodeDeploy`ist eine AWSverwaltete Richtlinie, die: EC2-Zugriff auf den S3-Bucket zum Herunterladen der Revision bietet. Diese -Funktion wird vom CodeDeploy Agenten auf EC2-Instances benötigt.

Verwenden dieser -Richtlinie

Sie können`AmazonEC2RoleforAWSCodeDeploy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 19. Mai 2015, 18:10 UTC
- Bearbeitete Zeit: 20. März 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2RoleforAWSCodeDeployLimited

`AmazonEC2RoleforAWSCodeDeployLimited`dist eine AWSverwaltete Richtlinie, die: Beschränkten EC2-Zugriff auf den S3-Bucket zum Herunterladen der Revision bietet. Diese -Funktion wird vom CodeDeploy Agenten auf EC2-Instances benötigt.

Verwenden dieser -Richtlinie

Sie können`AmazonEC2RoleforAWSCodeDeployLimited` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 24. August 2020, 17:55 UTC
- Bearbeitete Zeit: 20. Januar 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2RoleforDataPipelineRole

`AmazonEC2RoleforDataPipelineRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Servicerolle Amazon EC2 Role for Data Pipeline.

Verwenden dieser -Richtlinie

Sie können`AmazonEC2RoleforDataPipelineRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 22. Februar 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete -verwaltete -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2RoleforSSM

`AmazonEC2RoleforSSM`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie wird bald veraltet sein. Verwenden Sie dieManagedInstanceCore Richtlinie AmazonSSMManageSSMManaged, um dieAWS Systems Manager -Service-Core-Funktionalität auf EC2-Instances zu aktivieren. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile .html

Verwenden dieser -Richtlinie

Sie können`AmazonEC2RoleforSSM` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 29. Mai 2015, 17:48 UTC
- Bearbeitete Zeit: 24. Januar 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die -Standardversion der -Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2RolePolicyForLaunchWizard

`AmazonEC2RolePolicyForLaunchWizard`ist eine AWSverwaltete Richtlinie, die: Verwaltete Richtlinie für die LaunchWizard Amazon-Servicerolle für EC2

Verwenden dieser -Richtlinie

Sie können`AmazonEC2RolePolicyForLaunchWizard` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. November 2019, 08:05 UTC
- Bearbeitete Zeit: 16. Mai 2022, 21:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Version der Richtlinie

Version der Richtlinie:v10 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2SpotFleetAutoscaleRole

`AmazonEC2SpotFleetAutoscaleRole`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung der automatischen Skalierung für Amazon EC2 Spot Fleet

Verwenden dieser Richtlinie

Sie können`AmazonEC2SpotFleetAutoscaleRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 19. August 2016, 18:27 UTC
- Bearbeitete Zeit: 18. Februar 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEC2SpotFleetTaggingRole

`AmazonEC2SpotFleetTaggingRole`ist eine AWSverwaltete Richtlinie, die: Es EC2 Spot Fleet ermöglicht, Spot-Instances in Ihrem Namen anzufordern, zu beenden und zu taggen.

Verwenden dieser -Richtlinie

Sie können`AmazonEC2SpotFleetTaggingRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 29. Juni 2017, 18:19 UTC
- Bearbeitete Zeit: 23. April 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonECS_FullAccess

`AmazonECS_FullAccess`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff auf Amazon ECS-Ressourcen bietet und ECS-Funktionen durch Zugriff auf andereAWS Service-Ressourcen, einschließlich VPCs, Auto Scaling Scaling-Gruppen und CloudFormation Stacks, aktiviert.

Verwenden dieser Richtlinien

Sie können`AmazonECS_FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. November 2017 21:36 UTC
- Bearbeitete Zeit: 4. Januar 2023, 16:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Version der Richtlinie

Version der Richtlinie:v20 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` ist eine -AWSverwaltete Richtlinie, die: Bietet Administratorzugriff auf Private Certificate Authority, AWS Secrets Manager und andere , die für die Verwaltung von ECS-Service-Connect-TLS-Funktionen in Ihrem Namen AWS-Services erforderlich sind.

Verwenden dieser Richtlinie

Sie können `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 19. Januar 2024, 20:08 UTC
- Bearbeitungszeit: 19. Januar 2024, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRolePolicyForVolumes

`AmazonECSInfrastructureRolePolicyForVolumes` ist eine von AWS verwaltete Richtlinie, die: Bietet Zugriff auf andere -AWSServiceressourcen, die für die Verwaltung von Volumes erforderlich sind, die mit ECS-Workloads in Ihrem Namen verknüpft sind.

Verwenden dieser Richtlinie

Sie können `AmazonECSInfrastructureRolePolicyForVolumes` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 10. Januar 2024, 22:56 UTC
- Bearbeitungszeit: 10. Januar 2024, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonECSServiceRolePolicy

`AmazonECSServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die es Amazon ECS ermöglicht, Ihren Cluster zu verwalten.

Diese Richtlinie verwenden

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. Oktober 2017, 01:18 Uhr UTC
- Bearbeitete Zeit: 4. Dezember 2023, 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSTaskExecutionRolePolicy

`AmazonECSTaskExecutionRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf andereAWS -Serviceressourcen ermöglicht, die zum Ausführen von Amazon ECS-Aufgaben erforderlich sind

Verwenden dieser Richtlinie

Sie können`AmazonECSTaskExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 16. November 2017, 18:48 UTC
- Bearbeitete Zeit: 16. November 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEFSCSIDriverPolicy

`AmazonEFSCSIDriverPolicy`ist einAWSverwaltete Richtliniedas: Bietet Verwaltungszugriff auf EFS-Ressourcen und Lesezugriff auf EC2

Verwendung dieser Richtlinie

Sie können anhängen`AmazonEFSCSIDriverPolicy`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Servicerollen
- Zeit der Erstellung: 25. Juli 2023, 20:10 Uhr UTC
- Uhrzeit der Bearbeitung:25. Juli 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonEKS_CNI_Policy

`AmazonEKS_CNI_Policy` ist eine von AWS verwaltete Richtlinie, die: Diese Richtlinie stellt dem Amazon-VPC-CNI-Plugin (amazon-vpc-cni-k8s) die Berechtigungen bereit, die es zum Ändern der IP-Adresskonfiguration auf Ihren EKS-Worker-Knoten benötigt. Dieser Berechtigungssatz ermöglicht

es der CNI, Elastic Network Interfaces in Ihrem Namen aufzulisten, zu beschreiben und zu ändern. Weitere Informationen zum AWS VPC-CNI-Plugin finden Sie hier: https://github.com/aws/amazon-vpc-cni-k8s

Verwenden dieser Richtlinie

Sie können `AmazonEKS_CNI_Policy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:07 UTC
- Bearbeitungszeit: 04. März 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Richtlinienversion

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonEKSClusterPolicy

`AmazonEKSClusterPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Kubernetes die Berechtigungen, die es benötigt, um Ressourcen in Ihrem Namen zu verwalten. Kubernetes benötigt Ec2:CreateTags -Berechtigungen, um identifizierende Informationen auf EC2-Ressourcen zu platzieren, einschließlich, aber nicht beschränkt auf Instances, Sicherheitsgruppen und Elastic Network Interfaces.

Verwenden dieser -Richtlinie

Sie könnenAmazonEKSClusterPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2018 21:06 UTC
- Bearbeitete Zeit: 7. Februar 2023, 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEKSConnectorServiceRolePolicy

`AmazonEKSConnectorServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es Amazon EKS,AWS Ressourcen für den EKS-Connector zu verwalten

Verwenden von diese Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 4. September 2021, 20:31 UTC
- Bearbeitete Zeit: 4. September 2021, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEKSFargatePodExecutionRolePolicy

`AmazonEKSFargatePodExecutionRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf andereAWS -Serviceressourcen ermöglicht, die zum Ausführen von Amazon EKS-Pods aufAWS Fargate erforderlich sind

Verwenden dieser Richtlinie

Sie können`AmazonEKSFargatePodExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. November 2019, 04:34 UTC
- Bearbeitete Zeit: 22. November 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEKSForFargateServiceRolePolicy

`AmazonEKSForFargateServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie erteilt Amazon EKS die erforderlichen Berechtigungen zum Ausführen von Fargate-Aufgaben

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 22. November 2019, 04:36 UTC
- Bearbeitete Zeit: 22. November 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEKSLocalOutpostClusterPolicy

`AmazonEKSLocalOutpostClusterPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen für die Steuerungsebeneninstanzen des lokalen EKS-Clusters, die in Ihrem Konto ausgeführt werden, um Ressourcen in Ihrem Namen zu verwalten.

Verwenden dieser -Richtlinie

Sie können`AmazonEKSLocalOutpostClusterPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. August 2022, 21:56 UTC
- Bearbeitete Zeit: 17. Oktober 2022, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete Version ist die -verwaltete Version, die die Berechtigungen für die -verwaltete -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für

den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEKSLocalOutpostServiceRolePolicy

`AmazonEKSLocalOutpostServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es Amazon EKS Local ermöglicht,AWS Dienste in Ihrem Namen anzurufen.

Using this policy

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die die die die die die die die die Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 23...
- Bearbeitete Zeit: 24. Oktober 2022, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richt

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS

AmazonEKSServicePolicy

`AmazonEKSServicePolicy`ist eine AWS-verwaltete Richtlinie, die: Diese Richtlinie ermöglicht Amazon Elastic Container Service for Kubernetes, die erforderlichen Ressourcen für den Betrieb von EKS-Clustern zu erstellen und zu verwalten.

Verwenden dieser Richtlinie

Sie können`AmazonEKSServicePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2018 21:08 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEKSServiceRolePolicy

`AmazonEKSServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Eine Service-Linked Role ist erforderlich, damit Amazon EKSAWS Dienste in Ihrem Namen aufrufen kann.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. Februar 2020, 20:10 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEKSVPCResourceController

`AmazonEKSVPCResourceController`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die vom VPC Resource Controller zur Verwaltung von ENI und IPs für Worker-Knoten verwendet wird.

Verwenden dieser Richtlinien

Sie können`AmazonEKSVPCResourceController` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 12. August 2020, 00:55 UTC
- Bearbeitete Zeit: 12. August 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEKSWorkerNodePolicy

`AmazonEKSWorkerNodePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es Amazon EKS-Worker-Knoten, sich mit Amazon EKS-Clustern zu verbinden.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEKSWorkerNodePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:09 UTC
- Bearbeitete Zeit: 27. November 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElastiCacheFullAccess

`AmazonElastiCacheFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon ElastiCache über die bietetAWS Management Console.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElastiCacheFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 28. November 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElastiCacheReadOnlyAccess

`AmazonElastiCacheReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht Lesezugriff auf Amazon ElastiCache über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonElastiCacheReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticContainerRegistryPublicFullAccess

`AmazonElasticContainerRegistryPublicFullAccess`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff auf öffentliche Ressourcen von Amazon ECR gewährt

Verwenden dieser -Richtlinie

Sie könnenAmazonElasticContainerRegistryPublicFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2020, 17:25 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten verwaltete

AmazonElasticContainerRegistryPublicPowerUser

`AmazonElasticContainerRegistryPublicPowerUser`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf öffentliche Amazon ECR Repositorys bietet, das Löschen von Repositorys oder Richtlinienänderungen jedoch nicht zulässt.

Verwenden dieser Richtlinie

Sie können`AmazonElasticContainerRegistryPublicPowerUser` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2020, 16:16 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die -verwaltete Richtlinie, die die Berechtigungen für die -verwaltete Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticContainerRegistryPublicReadOnly

`AmazonElasticContainerRegistryPublicReadOnly`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf öffentliche Amazon ECR Repositorys gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonElasticContainerRegistryPublicReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2020, 17:27 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticFileSystemClientFullAccess

`AmazonElasticFileSystemClientFullAccess`ist eine AWSverwaltete Richtlinie, die: Root-Client-Zugriff auf ein Amazon EFS-Dateisystem gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonElasticFileSystemClientFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. Januar 2020, 16:27 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticFileSystemClientReadOnlyAccess

`AmazonElasticFileSystemClientReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Einen schreibgeschützten Client-Zugriff auf ein Amazon EFS-Dateisystem gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonElasticFileSystemClientReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. Januar 2020, 16:24 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticFileSystemClientReadWriteAccess

`AmazonElasticFileSystemClientReadWriteAccess`ist eine AWSverwaltete Richtlinie, die: Lese- und Schreibclientzugriff auf ein Amazon EFS-Dateisystem bereitstellt

Verwenden dieser -Richtlinie

Sie können`AmazonElasticFileSystemClientReadWriteAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. Januar 2020, 16:21 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AmazonElasticFileSystemFullAccess

`AmazonElasticFileSystemFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon EFS über die bietetAWS Management Console.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonElasticFileSystemFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2015, 16:22 UTC
- Bearbeitete Zeit: 28. November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemReadOnlyAccess

`AmazonElasticFileSystemReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon EFS über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonElasticFileSystemReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2015, 16:25 UTC
- Bearbeitete Zeit: 10. Januar 2022, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -verwaltete -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticFileSystemServiceRolePolicy

`AmazonElasticFileSystemServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Elastic File System ermöglicht,AWS Ressourcen in Ihrem Namen zu verwalten

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 5. November 2019, 16:52 UTC
- Bearbeitete Zeit: 10. Januar 2022, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der Richtlinie ist die Version ermöglicht, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticFileSystemsUtils

`AmazonElasticFileSystemsUtils`ist eine AWSverwaltete Richtlinie, die: Es Kunden ermöglicht,AWS Systems Manager zu verwenden, um das Amazon EFS Utilities (amazon-efs-utils) - Paket auf ihren EC2-Instances automatisch zu verwalten und sie CloudWatchLog zu verwenden, um

Benachrichtigungen über die erfolgreiche oder fehlgeschlagene Installation des EFS-Dateisystems zu erhalten.

Verwenden dieser Richtlinie

Sie können`AmazonElasticFileSystemsUtils` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. September 2020, 15:16 UTC
- Bearbeitete Zeit: 29. September 2020, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticMapReduceEditorsRole

`AmazonElasticMapReduceEditorsRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Amazon Elastic MapReduce Editors-Servicerolle.

Verwenden dieser -Richtlinie

Sie können`AmazonElasticMapReduceEditorsRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Erstellungszeit: 16. November 2018, 21:55 UTC

- Bearbeitete Zeit: 9. Februar 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -verwaltete -verwaltete -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticMapReduceforAutoScalingRole

`AmazonElasticMapReduceforAutoScalingRole`ist eine AWSverwaltete Richtlinie, die: Amazon Elastic MapReduce for Auto Scaling. Rolle, mit der Auto Scaling Instances zu Ihrem EMR-Cluster hinzufügen und daraus entfernen kann.

Verwenden dieser -Richtlinie

Sie können`AmazonElasticMapReduceforAutoScalingRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie

- Aufnahmezeit: 18. November 2016, 01:09 UTC
- Bearbeitete Zeit: 18. November 2016, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticMapReduceforEC2Role

`AmazonElasticMapReduceforEC2Role`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Amazon Elastic MapReduce for EC2-Servicerolle.

Verwenden dieser -Richtlinien

Sie können`AmazonElasticMapReduceforEC2Role` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 11. August 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die Berechtigungen für die Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IRichtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalRichtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticMapReduceFullAccess

`AmazonElasticMapReduceFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist veraltet. Eine Anleitung finden Sie in der Dokumentation: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html. Bietet vollen Zugriff auf Amazon Elastic MapReduce und die zugrundeliegenden Dienste, die es benötigt, wie EC2 und S3

Verwenden dieser -Richtlinie

Sie können`AmazonElasticMapReduceFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 11. Oktober 2019, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticMapReducePlacementGroupPolicy

`AmazonElasticMapReducePlacementGroupPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die es EMR ermöglicht, EC2-Platzierungsgruppen zu erstellen, zu beschreiben und zu löschen.

Verwenden dieser Richtlinie

Sie können`AmazonElasticMapReducePlacementGroupPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. September 2020, 00:37 UTC
- Bearbeitete Zeit: 29. September 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AmazonElasticMapReduceReadOnlyAccess

`AmazonElasticMapReduceReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon Elastic MapReduce über dieAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AmazonElasticMapReduceReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 29. Juli 2020, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AmazonElasticMapReduceRole

`AmazonElasticMapReduceRole`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist veraltet. Eine Anleitung finden Sie in der Dokumentation: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html. Standardrichtlinie für die Amazon MapReduce Elastic-Servicerolle.

Verwenden dieser -Richtlinie

Sie können`AmazonElasticMapReduceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 24. Juni 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Version der Richtlinie

Version der Richtlinie:v10 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticsearchServiceRolePolicy

`AmazonElasticsearchServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Elasticsearch Service den Zugriff auf andere AWS Services wie EC2 Networking APIs in Ihrem Namen ermöglicht.

Diese Richtlinie verwenden

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Juli 2017, 00:15 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoder_FullAccess

`AmazonElasticTranscoder_FullAccess`ist eine AWSverwaltete Richtlinie, die: Benutzern vollen Zugriff auf Elastic Transcoder und den Zugriff auf die zugehörigen Dienste gewährt, der für die vollständige Funktionalität von Elastic Transcoder erforderlich ist.

Verwenden dieser -Richtlinie

Sie können`AmazonElasticTranscoder_FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. April 2018, 18:59 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticTranscoder_JobsSubmitter

`AmazonElasticTranscoder_JobsSubmitter`ist eine AWSverwaltete Richtlinie, die: Benutzern die Berechtigung erteilt, Voreinstellungen zu ändern, Jobs einzureichen und Elastic Transcoder Transcoder-Einstellungen einzusehen. Diese Richtlinie gewährt auch einen gewissen Lesezugriff auf einige andere Dienste, die für die Verwendung der Elastic Transcode-Konsole erforderlich sind, darunter S3, IAM und SNS.

Verwenden dieser -Richtlinie

Sie können`AmazonElasticTranscoder_JobsSubmitter` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Juni 2018, 21:12 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticTranscoder_ReadOnlyAccess

`AmazonElasticTranscoder_ReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Benutzern Lesezugriff auf Elastic Transcoder und Listenzugriff auf verwandte Dienste gewährt.

Verwenden dieser Richtlinien

Sie können`AmazonElasticTranscoder_ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Juni 2018, 21:09 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
```

```
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonElasticTranscoderRole

`AmazonElasticTranscoderRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Amazon Elastic Transcoder-Servicerolle.

Verwenden dieser Richtlinien

Sie können`AmazonElasticTranscoderRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 13. Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- ErsteAWS Schritte mit mit den geringsten Berechtigungen

AmazonEMRCleanupPolicy

`AmazonEMRCleanupPolicy`ist eine AWSverwaltete Richtlinie, die: Ermöglicht die Aktionen, die EMR zum Beenden und Löschen vonAWS EC2-Ressourcen benötigt, wenn die EMR-Dienstrolle diese Fähigkeit verloren hat.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. September 2017, 23:54 UTC
- Bearbeitete Zeit: 29. September 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion ist die Version, die die die Durchführung der Berechtigungen für die Richtlinie definiert, die die die Durchführung der Berechtigungen definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEMRContainersServiceRolePolicy

`AmazonEMRContainersServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf andereAWS Serviceressourcen ermöglicht, die für die Ausführung von Amazon EMR erforderlich sind

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 9. Dezember 2020, 00:38 UTC
- Bearbeitete Zeit: 10. März 2023, 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardlinien-Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEMRFullAccessPolicy_v2

`AmazonEMRFullAccessPolicy_v2`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff auf Amazon EMR

Verwendung dieser Richtlinie

Sie können anhängen`AmazonEMRFullAccessPolicy_v2`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 12. März 2021, 01:50 Uhr UTC
- Uhrzeit der Bearbeitung:28. Juli 2023, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Version der Richtlinie

Version der Richtlinie: v4(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonEMRReadOnlyAccessPolicy_v2

`AmazonEMRReadOnlyAccessPolicy_v2`ist einAWSverwaltete Richtliniedas: Bietet schreibgeschützten Zugriff auf Amazon EMR und die zugehörigenCloudWatchMetriken.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonEMRReadOnlyAccessPolicy_v2`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 12. März 2021, 01:39 Uhr UTC
- Uhrzeit der Bearbeitung:02. August 2023, 19:15 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Version der Richtlinie

Version der Richtlinie: v3(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonEMRServerlessServiceRolePolicy

`AmazonEMRServerlessServiceRolePolicy` ist eine -AWSverwaltete Richtlinie, die: Ermöglicht den Zugriff auf andere -AWSServiceressourcen, die zum Ausführen von Amazon EMRServerless erforderlich sind

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 20. Mai 2022, 23:15 UTC
- Bearbeitungszeit: 25. Januar 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonEMRServicePolicy_v2

`AmazonEMRServicePolicy_v2`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie wird für die Amazon EMR Service Role verwendet und sollte NICHT für andere IAM-Benutzer oder -Rollen in

Ihrem Konto verwendet werden. Die Richtlinie gewährt Berechtigungen zur Erstellung und Verwaltung von Ressourcen im Zusammenhang mit EMR und zugehörigen Diensten, die für den Betrieb Ihres EMR-Clusters erforderlich sind.

Verwenden dieser -Richtlinie

Sie können`AmazonEMRServicePolicy_v2` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 12. März 2021, 01:11 UTC
- Bearbeitete Zeit: 15. Februar 2022, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Standardversion definiert die Berechtigungen für die -Standardrichtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonESCognitoAccess

`AmazonESCognitoAccess`ist eine AWSverwaltete Richtlinie, die: eingeschränkten Zugriff auf den Amazon Cognito Cognito-Konfigurationsservice bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonESCognitoAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. Februar 2018, 22:29 UTC
- Bearbeitete Zeit: 20. Dezember 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonESFullAccess

`AmazonESFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den Amazon ES-Konfigurationsservice bietet.

Verwenden dieser Richtlinien

Sie können`AmazonESFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Oktober 2015, 19:14 UTC
- Bearbeitete Zeit: 1. Oktober 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
        "es:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen mit den Berechtigungen mit den Einstellungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen Berechtigungen

AmazonESReadOnlyAccess

`AmazonESReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf den Amazon ES-Konfigurationsservice gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonESReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Oktober 2015, 19:18 UTC
- Bearbeitete Zeit: 3. Oktober 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgeApiDestinationsServiceRolePolicy

`AmazonEventBridgeApiDestinationsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Ermöglicht EventBridge den Zugriff auf Secret Manager-Ressourcen in Ihrem Namen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 11. Februar 2021, 20:52 UTC
- Bearbeitete Zeit: 11. Februar 2021, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
```

```
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgeFullAccess

`AmazonEventBridgeFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon bietet EventBridge.

Verwenden dieser -Richtlinie

Sie können`AmazonEventBridgeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Juli 2019, 14:08 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von Berechtigungen für die geringsten
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -Richtlinien und Umstellung auf Berechtigungen mit Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgePipesFullAccess

`AmazonEventBridgePipesFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon EventBridge Pipes bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonEventBridgePipesFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2022, 17:03 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Richtlinien und definiert die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf auf auf auf auf auf auf auf auf auf auf auf auf auf auf mit den geringsten Berechtigungen

AmazonEventBridgePipesOperatorAccess

`AmazonEventBridgePipesOperatorAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff und Operator-Zugriff (Möglichkeit, Pipes zu stoppen und zu starten) auf Amazon EventBridge Pipes bereitstellt.

Verwenden dieser -Richtlinie

Sie können`AmazonEventBridgePipesOperatorAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2022, 17:04 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Standard-Standardrichtlinie definiert die Berechtigungen für die -Standard-Standard-Standard-Standard-Standard-Standard-Standard-Standard-Standardversion Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgePipesReadOnlyAccess

`AmazonEventBridgePipesReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon EventBridge Pipes gewährt.

Verwenden dieser -diese -Richtlinie

Sie können`AmazonEventBridgePipesReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2022, 17:04 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standard-Richtlinie definiert die -Standardversion der -Standard-Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AmazonEventBridgeReadOnlyAccess

`AmazonEventBridgeReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon gewährt EventBridge.

Verwenden dieser -Richtlinie

Sie können`AmazonEventBridgeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Juli 2019, 13:59 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgeSchedulerFullAccess

`AmazonEventBridgeSchedulerFullAccess`ist eine AWSverwaltete Richtlinie, die: Die AmazonEventBridgeSchedulerFullAccess verwaltete Richtlinie gewährt Berechtigungen zur Verwendung aller EventBridge Scheduler-Aktionen für Zeitpläne und Zeitplangruppen.

Verwenden dieser -Richtlinie

Sie können`AmazonEventBridgeSchedulerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 10. November 2022, 18:37 UTC
- Bearbeitete Zeit: 10. November 2022, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgeSchedulerReadOnlyAccess

`AmazonEventBridgeSchedulerReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Die AmazonEventBridgeSchedulerReadOnlyAccess verwaltete Richtlinie gewährt Leserechte zum Anzeigen von Details zu Ihren Zeitplänen und Zeitplangruppen

Verwenden dieser Richtlinie

Sie können`AmazonEventBridgeSchedulerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 10. November 2022, 18:50 UTC
- Bearbeitete Zeit: 10. November 2022, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgeSchemasFullAccess

`AmazonEventBridgeSchemasFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon EventBridge Schemas bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonEventBridgeSchemasFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. November 2019, 23:12 UTC
- Bearbeitete Zeit: 28. November 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion definiert die Berechtigungen für die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgeSchemasReadOnlyAccess

`AmazonEventBridgeSchemasReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon EventBridge Schemas gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonEventBridgeSchemasReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. November 2019, 23:05 UTC
- Bearbeitete Zeit: 1. Mai 2020, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonEventBridgeSchemasServiceRolePolicy

`AmazonEventBridgeSchemasServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen für verwaltete Regeln gewährt, die von EventBridge Amazon-Schemas erstellt wurden.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 27. November 2019, 01:10 UTC
- Bearbeitete Zeit: 27. November 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtdokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonFISServiceRolePolicy

`AmazonFISServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Eine Richtlinie, die es derAWS FIS ermöglicht, die Überwachung und die Ressourcenauswahl für Experimente zu verwalten.

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. Dezember 2020, 21:18 UTC

- Bearbeitete Zeit: 25. Oktober 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinien

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalteter Richtlinien und Umstellung auf Berechtigungen

AmazonForecastFullAccess

`AmazonForecastFullAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf alle Aktionen für Amazon Forecast gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonForecastFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Januar 2019, 01:52 UTC
- Bearbeitete Zeit: 18. Januar 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AmazonFraudDetectorFullAccessPolicy

`AmazonFraudDetectorFullAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf alle Aktionen für Amazon Fraud Detector gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonFraudDetectorFullAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 22:46 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonFreeRTOSFullAccess

`AmazonFreeRTOSFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollständige Zugriffsrichtlinie für Amazon FreeRTOS

Verwenden dieser -verwaltete Richtlinien

Sie können`AmazonFreeRTOSFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2017, 15:32 UTC
- Bearbeitete Zeit: 29. November 2017, 15:32 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonFreeRTOSOTAUpdate

`AmazonFreeRTOSOTAUpdate`ist eine AWSverwaltete Richtlinie, die: Benutzern den Zugriff auf Amazon FreeRTOS OTA Update ermöglicht

Verwenden dieser -Richtlinie

Sie könnenAmazonFreeRTOSOTAUpdate an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 27. August 2018, 22:43 UTC
- Bearbeitete Zeit: 18. Dezember 2020, 17:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonFSxConsoleFullAccess

`AmazonFSxConsoleFullAccess` ist eine von AWS verwaltete Richtlinie, die: Vollzugriff auf Amazon FSx und Zugriff auf verwandte -AWSServices über die ermöglichtAWS Management Console.

Verwenden dieser Richtlinie

Sie können `AmazonFSxConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:36 UTC
- Bearbeitungszeit: 10. Januar 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Richtlinienversion

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonFSxConsoleReadOnlyAccess

`AmazonFSxConsoleReadOnlyAccess` ist eine -AWSverwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf Amazon FSx und Zugriff auf verwandte -AWSServices über die AWS Management Console.

Verwenden dieser Richtlinie

Sie können `AmazonFSxConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:35 UTC
- Bearbeitungszeit: 10. Januar 2024, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen

- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonFSxFullAccess

`AmazonFSxFullAccess` ist eine von AWS verwaltete Richtlinie, die: Vollzugriff auf Amazon FSx und Zugriff auf verwandte -AWSServices bietet.

Verwenden dieser Richtlinie

Sie können `AmazonFSxFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:34 UTC
- Bearbeitungszeit: 10. Januar 2024, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Richtlinienversion

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonFSxReadOnlyAccess

`AmazonFSxReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon FSx gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonFSxReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. November 2018, 16:33 UTC
- Bearbeitete Zeit: 28. November 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonFSxServiceRolePolicy

`AmazonFSxServiceRolePolicy` ist eine -AWSverwaltete Richtlinie, die: Ermöglicht Amazon FSx, -AWSRessourcen in Ihrem Namen zu verwalten

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 28. November 2018, 10:38 UTC
- Bearbeitungszeit: 10. Januar 2024, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonGlacierFullAccess

`AmazonGlacierFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Glacier über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonGlacierFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonGlacierReadOnlyAccess

`AmazonGlacierReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon Glacier über dieAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AmazonGlacierReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 5. Mai 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonGrafanaAthenaAccess

`AmazonGrafanaAthenaAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Zugriff auf Amazon Athena und die Abhängigkeiten, die erforderlich sind, um das Abfragen und Schreiben von Ergebnissen aus dem Amazon Athena-Plugin in Amazon Grafana in S3 zu ermöglichen.

Verwenden dieser Richtlinie

Sie können`AmazonGrafanaAthenaAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 22. November 2021, 17:11 UTC
- Bearbeitete Zeit: 22. November 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonGrafanaCloudWatchAccess

`AmazonGrafanaCloudWatchAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Zugriff auf Amazon CloudWatch und die Abhängigkeiten, die für die Verwendung CloudWatch als Datenquelle innerhalb von Amazon Managed Grafana erforderlich sind.

Verwenden dieser -Richtlinie

Sie können`AmazonGrafanaCloudWatchAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 24. März 2023, 22:41 UTC
- Bearbeitete Zeit: 24. März 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonGrafanaRedshiftAccess

`AmazonGrafanaRedshiftAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt eingeschränkten Zugriff auf Amazon Redshift und die Abhängigkeiten, die für die Verwendung des Amazon Redshift Redshift-Plug-ins in Amazon Grafana erforderlich sind.

Verwenden dieser -Richtlinie

Sie können`AmazonGrafanaRedshiftAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 26. November 2021, 23:15 UTC
- Bearbeitete Zeit: 26. November 2021, 23:15 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonGrafanaServiceLinkedRolePolicy

`AmazonGrafanaServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff aufAWS Ressourcen bietet, die von Amazon Grafana verwaltet oder verwendet werden.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 8. November 2022, 23:10 UTC
- Bearbeitete Zeit: 8. November 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Durchführung von Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonGuardDutyFullAccess

`AmazonGuardDutyFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf die Nutzung von Amazon bietet GuardDuty.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGuardDutyFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 22:31 UTC
- Bearbeitete Zeit: 16. November 2023, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyMalwareProtectionServiceRolePolicy

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: GuardDuty Malware Protection die serviceverknüpfte Rolle (SLR) namens verwendet AWSServiceRoleForAmazonGuardDutyMalwareProtection. Diese serviceverknüpfte Rolle ermöglicht es dem GuardDuty Malware-Schutz, agentenlose Scans durchzuführen, um Malware zu erkennen. Es ermöglicht GuardDuty , Snapshots in Ihrem Konto zu erstellen und die Snapshots für das GuardDuty Servicekonto freizugeben, um nach Malware zu suchen. Es wertet diese freigegebenen Snapshots aus und schließt die abgerufenen EC2-Instance-Metadaten in die Erkenntnisse von GuardDuty Malware Protection ein. Die AWSServiceRoleForAmazonGuardDutyMalwareProtection serviceverknüpfte Rolle vertraut dem malware-protection.guardduty.amazonaws.com-Service, die Rolle zu übernehmen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 19. Juli 2022, 19:06 Uhr UTC
- Bearbeitungszeit: 25. Januar 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonGuardDutyReadOnlyAccess

`AmazonGuardDutyReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf GuardDuty Amazon-Ressourcen gewährt

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGuardDutyReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 22:29 Uhr UTC
- Bearbeitete Zeit: 16. November 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyServiceRolePolicy

`AmazonGuardDutyServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Zugriff auf von Amazon Guard verwendete oder verwaltete AWS Ressourcen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 28. November 2017, 20:12 UTC
- Bearbeitungszeit: 09. Februar 2024, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonHealthLakeFullAccess

`AmazonHealthLakeFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den HealthLake Amazon-Service bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonHealthLakeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 17. Februar 2021, 01:07 UTC
- Bearbeitete Zeit: 17. Februar 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonHealthLakeReadOnlyAccess

`AmazonHealthLakeReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf den HealthLake Amazon-Service gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonHealthLakeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. Februar 2021, 02:43 UTC
- Bearbeitete Zeit: 17. Februar 2021, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonHoneycodeFullAccess

`AmazonHoneycodeFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Honeycode über dasAWS Management Console und das SDK bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonHoneycodeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 24. Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonHoneycodeReadOnlyAccess

`AmazonHoneycodeReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Über dasAWS Management Console und das SDK nur Lesezugriff auf Honeycode bietet.

Verwenden dieser Richtlinie

Sie können`AmazonHoneycodeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonHoneycodeServiceRolePolicy

`AmazonHoneycodeServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Eine serviceverknüpfte Rolle, die Amazon Honeycode für den Zugriff auf Ihre Ressourcen benötigt.

Verwenden Sie diese Richtlinie Richtlinie Richtlinie Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. November 2020, 18:03 UTC
- Bearbeitete Zeit: 18. November 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen

AmazonHoneycodeTeamAssociationFullAccess

`AmazonHoneycodeTeamAssociationFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die Honeycode Team Association über dasAWS Management Console und das SDK bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonHoneycodeTeamAssociationFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2020, 20:28 UTC

- Bearbeitete Zeit: 24. Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AmazonHoneycodeTeamAssociationReadOnlyAccess

`AmazonHoneycodeTeamAssociationReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Über dasAWS Management Console und das SDK nur Lesezugriff auf die Honeycode Team Association bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonHoneycodeTeamAssociationReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2020, 20:27 UTC
- Bearbeitete Zeit: 24. Juni 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Version ist die -verwaltete Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonHoneycodeWorkbookFullAccess

`AmazonHoneycodeWorkbookFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Honeycode Workbook über dasAWS Management Console und das SDK bietet.

Verwenden dieser Richtlinien

Sie können`AmazonHoneycodeWorkbookFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonHoneycodeWorkbookReadOnlyAccess

`AmazonHoneycodeWorkbookReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Über dasAWS Management Console und das SDK nur Lesezugriff auf Honeycode Workbook bietet.

Verwenden dieser Richtlinie

Sie könnenAmazonHoneycodeWorkbookReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Standardrichtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AmazonInspector2AgentlessServiceRolePolicy

`AmazonInspector2AgentlessServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Inspector Zugriff auf Sicherheitsbewertungen gewährt, die für die Durchführung ohne Agenten AWS-Services erforderlich sind

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. November 2023, 15:18 UTC
- Bearbeitete Zeit: 20. November 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2FullAccess

`AmazonInspector2FullAccess`ist einAWSverwaltete RichtlinieDas: Bietet vollen Zugriff auf Amazon Inspector und Zugriff auf andere verwandte Dienste wie Organisationen.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonInspector2FullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 29. November 2021, 19:10 Uhr UTC
- Uhrzeit der Bearbeitung:03. August 2023, 19:28 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Version der Richtlinie

Version der Richtlinie: v3(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "inspector2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonInspector2ManagedCisPolicy

`AmazonInspector2ManagedCisPolicy` ist eine von AWS verwaltete Richtlinie, die: Dies ist eine von verwaltete Richtlinie, die Kunden ihren Rollen anfügen sollten, um mit dem Inspector-Service für CIS-Scans zu kommunizieren

Verwenden dieser Richtlinie

Sie können `AmazonInspector2ManagedCisPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 24. Januar 2024, 16:31 UTC
- Bearbeitungszeit: 24. Januar 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonInspector2ReadOnlyAccess

`AmazonInspector2ReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf den Amazon Inspector2-Service und die entsprechenden Support-Services gewährt

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonInspector2ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Januar 2022, 14:45 UTC
- Bearbeitete Zeit: 22. September 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2ServiceRolePolicy

`AmazonInspector2ServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Gewährt Amazon Inspector Zugriff auf , die für die Durchführung von Sicherheitsbewertungen AWS-Services erforderlich sind

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 16. November 2021, 20:27 UTC
- Bearbeitungszeit: 22. Januar 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonInspectorFullAccess

`AmazonInspectorFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Inspector bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonInspectorFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Oktober 2015, 17:08 UTC
- Bearbeitete Zeit: 21. Dezember 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und mit den geringsten Berechtigungen

AmazonInspectorReadOnlyAccess

`AmazonInspectorReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Inspector gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonInspectorReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Oktober 2015, 17:08 UTC
- Bearbeitete Zeit: 1. Oktober 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonInspectorServiceRolePolicy

`AmazonInspectorServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Inspector Zugriff auf die für die Durchführung von SicherheitsbewertungenAWS-Services erforderlichen Daten gewährt

Verwenden dieser Richtlinie dieser Richtlinie dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. November 2017, 15:48 UTC
- Bearbeitete Zeit: 11. September 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die Standardversion der Richtlinie ist die Version der Richtlinien für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

Dokument von JSON-Richtlinien von

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS verwalteter Richtlinien und Umstellung auf Berechtigungen verwalteter Richtlinien mit den geringsten Berechtigungen verwalteter Richtlinien von Richtlinien mit den geringsten Richtlinien

AmazonKendraFullAccess

`AmazonKendraFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Kendra über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonKendraFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 16:15 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonKendraReadOnlyAccess

`AmazonKendraReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon Kendra über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonKendraReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 16:13 UTC
- Bearbeitete Zeit: 27. Mai 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonKeyspacesFullAccess

`AmazonKeyspacesFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Keyspaces gewährt

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKeyspacesFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2020, 17:06 UTC
- Bearbeitete Zeit: 3. Oktober 2023, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKeyspacesReadOnlyAccess

`AmazonKeyspacesReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Keyspaces gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonKeyspacesReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. April 2020, 17:07 UTC
- Bearbeitete Zeit: 7. Juli 2022, 14:54 UTC

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

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonKeyspacesReadOnlyAccess_v2

`AmazonKeyspacesReadOnlyAccess_v2`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf Amazon Keyspaces und verwandte AWS Dienste gewährt.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKeyspacesReadOnlyAccess_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. September 2023, 17:01 UTC
- Bearbeitete Zeit: 12. September 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisAnalyticsFullAccess

`AmazonKinesisAnalyticsFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Kinesis Analytics über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonKinesisAnalyticsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. September 2016, 19:01 UTC
- Bearbeitete Zeit: 21. September 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AmazonKinesisAnalyticsReadOnly

`AmazonKinesisAnalyticsReadOnly`ist eine AWSverwaltete Richtlinie, die: Ermöglicht Lesezugriff auf Amazon Kinesis Analytics über dieAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AmazonKinesisAnalyticsReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. September 2016, 18:16 UTC
- Bearbeitete Zeit: 21. September 2016, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonKinesisFirehoseFullAccess

`AmazonKinesisFirehoseFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf alle Amazon Kinesis Firehose Delivery Streams bietet.

Verwenden dieser Richtlinien

Sie können`AmazonKinesisFirehoseFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Oktober 2015, 18:45 UTC
- Bearbeitete Zeit: 7. Oktober 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonKinesisFirehoseReadOnlyAccess

`AmazonKinesisFirehoseReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf alle Amazon Kinesis Firehose Delivery Streams gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonKinesisFirehoseReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Oktober 2015, 18:43 UTC
- Bearbeitete Zeit: 7. Oktober 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonKinesisFullAccess

`AmazonKinesisFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alle Streams über die bietetAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonKinesisFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf den geringsten Berechtigungen und Umstellung auf den geringsten Berechtigungen und Umstellung auf den geringsten

AmazonKinesisReadOnlyAccess

`AmazonKinesisReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf alle Streams über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonKinesisReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonKinesisVideoStreamsFullAccess

`AmazonKinesisVideoStreamsFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Kinesis Video Streams über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonKinesisVideoStreamsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 1. Dezember 2017, 23:27 UTC
- Bearbeitete Zeit: 1. Dezember 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonKinesisVideoStreamsReadOnlyAccess

`AmazonKinesisVideoStreamsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Bietet nur Lesezugriff aufAWS Kinesis Video Streams über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie könnenAmazonKinesisVideoStreamsReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2017, 23:14 UTC
- Bearbeitete Zeit: 1. Dezember 2017, 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLaunchWizard_Fullaccess

`AmazonLaunchWizard_Fullaccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf denAWS Startassistenten und andere erforderliche Dienste.

Verwenden dieser Richtlinien

Sie können`AmazonLaunchWizard_Fullaccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. August 2020, 17:47 UTC
- Bearbeitete Zeit: 22. Februar 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Version der Richtlinie

Version der Richtlinie:v15 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLaunchWizardFullAccessV2

`AmazonLaunchWizardFullAccessV2`ist einAWSverwaltete Richtliniedas: Voller Zugriff aufAWSStarten Sie den Assistenten und andere erforderliche Dienste.

Verwenden Sie diese Richtlinie

Sie können anhängen`AmazonLaunchWizardFullAccessV2`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie
- Zeitpunkt der Erstellung: 01. September 2023, 17:14 Uhr UTC
- Bearbeitete Zeit:1. September 2023, 17:14 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonLexChannelsAccess

`AmazonLexChannelsAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es Kunden, Lex Runtime von Kanälen aus aufzurufen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 13. Januar 2021, 20:12 UTC
- Bearbeitete Zeit: 13. Januar 2021, 20:12 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die StandardVersion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-RichtRichtRichtlinien

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLexFullAccess

`AmazonLexFullAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf Amazon Lex über die AWS Management Console. Bietet auch Zugriff zum Erstellen von serviceverknüpften Lex-Rollen und zum Erteilen von Lex-Berechtigungen zum Aufrufen eines begrenzten Satzes von Lambda-Funktionen.

Verwenden dieser Richtlinie

Sie können `AmazonLexFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2017, 23:20 UTC
- Bearbeitungszeit: 07. Februar 2024, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Richtlinienversion

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
```

```
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement9",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
```

```
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lex.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement12",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "channels.lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLexReadOnly

`AmazonLexReadOnly`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Lex gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonLexReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. April 2017, 23:13 UTC
- Bearbeitete Zeit: 31. Januar 2023, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotRecommendation",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotRecommendations",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
```

```
        "lex:ListRecommendedIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLexReplicationPolicy

`AmazonLexReplicationPolicy` ist eine von AWS verwaltete Richtlinie, die Amazon Lex ermöglicht, Lex-Ressourcen regionsübergreifend in Ihrem Namen zu replizieren.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 31. Januar 2024, 23:29 UTC
- Bearbeitungszeit: 08. März 2024, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonLexRunBotsOnly

`AmazonLexRunBotsOnly`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Amazon Lex-Konversations-APIs bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonLexRunBotsOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. April 2017, 23:06 UTC
- Bearbeitete Zeit: 18. August 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLexV2BotPolicy

`AmazonLexV2BotPolicy`ist eine AWSverwaltete Richtlinie, die: Lex V2-Bots Zugriff gewährt, um in Ihrem Namen andereAWS Dienste anzurufen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 13. Januar 2021, 20:10 UTC
- Bearbeitete Zeit: 13. Januar 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die die die die die die Richtlinien für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONRichtliniendokument

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

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLookoutEquipmentFullAccess

`AmazonLookoutEquipmentFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den Betrieb von Amazon Lookout for Equipment bietet

Verwenden dieser -Richtlinie

Sie können`AmazonLookoutEquipmentFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. April 2021, 15:52 UTC
- Bearbeitete Zeit: 24. November 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete Version ist die -verwaltete -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf mit den geringsten sten sten sten sten sten sten sten sten sten sten sten sten sten sten

AmazonLookoutEquipmentReadOnlyAccess

`AmazonLookoutEquipmentReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Lookout for Equipments gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonLookoutEquipmentReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. Mai 2021, 16:47 UTC
- Bearbeitete Zeit: 10. November 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLookoutMetricsFullAccess

`AmazonLookoutMetricsFullAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf alle Aktionen für Amazon Lookout for Metrics gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonLookoutMetricsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Mai 2021, 00:43 UTC
- Bearbeitete Zeit: 7. Mai 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLookoutMetricsReadOnlyAccess

`AmazonLookoutMetricsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf alle schreibgeschützten Aktionen für Amazon Lookout for Metrics gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonLookoutMetricsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Mai 2021, 00:43 UTC
- Bearbeitete Zeit: 4. Januar 2022, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLookoutVisionConsoleFullAccess

`AmazonLookoutVisionConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Lookout for Vision und eingeschränkten Zugriff auf die erforderlichen Service- und Konsolenabhängigkeiten bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonLookoutVisionConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Mai 2021, 19:37 UTC
- Bearbeitete Zeit: 11. Mai 2021, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLookoutVisionConsoleReadOnlyAccess

`AmazonLookoutVisionConsoleReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Lookout for Vision und eingeschränkten Zugriff auf die erforderlichen Service- und Konsolenabhängigkeiten bietet.

Verwenden dieser Richtlinien

Sie können`AmazonLookoutVisionConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Mai 2021, 19:32 UTC
- Bearbeitete Zeit: 9. Dezember 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLookoutVisionFullAccess

`AmazonLookoutVisionFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Lookout for Vision und eingeschränkten Zugriff auf die erforderlichen Abhängigkeiten bietet.

Verwenden dieser Richtlinie

Sie können`AmazonLookoutVisionFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Mai 2021, 19:24 UTC
- Bearbeitete Zeit: 11. Mai 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonLookoutVisionReadOnlyAccess

`AmazonLookoutVisionReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Lookout for Vision und eingeschränkten Zugriff auf erforderliche Abhängigkeiten bietet.

Verwenden

Sie können`AmazonLookoutVisionReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Mai 2021, 19:11 UTC
- Bearbeitete Zeit: 9. Dezember 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AmazonMachineLearningBatchPredictionsAccess

`AmazonMachineLearningBatchPredictionsAccess`ist eine AWSverwaltete Richtlinie, die: Benutzern die Erlaubnis erteilt, Batch-Vorhersagen von Amazon Machine Learning anzufordern.

Verwenden dieser -verwaltete Richtlinien

Sie können`AmazonMachineLearningBatchPredictionsAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. April 2015, 17:12 UTC
- Bearbeitete Zeit: 9. April 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion definiert die Berechtigungen für die -verwaltete - Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMachineLearningCreateOnlyAccess

`AmazonMachineLearningCreateOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht den Zugriff auf Amazon Machine Learning Learning-Ressourcen, die nicht vorhersehbar sind.

Verwenden dieser Richtlinien

Sie können`AmazonMachineLearningCreateOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. April 2015, 17:18 UTC
- Bearbeitete Zeit: 29. Juni 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMachineLearningFullAccess

`AmazonMachineLearningFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Machine Learning Learning-Ressourcen bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonMachineLearningFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. April 2015, 17:25 UTC
- Bearbeitete Zeit: 9. April 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Benutzern die Erlaubnis erteilt, den Echtzeit-Endpunkt für Amazon Machine Learning Learning-Modelle zu erstellen und zu löschen.

Verwenden dieser Richtlinie

Sie können`AmazonMachineLearningManageRealTimeEndpointOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. April 2015, 17:32 UTC
- Bearbeitete Zeit: 9. April 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMachineLearningReadOnlyAccess

`AmazonMachineLearningReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Machine Learning Learning-Ressourcen gewährt.

Verwenden dieser Richtlinie

Sie können`AmazonMachineLearningReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. April 2015, 17:40 UTC
- Bearbeitete Zeit: 9. April 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen und Umstellung

AmazonMachineLearningRealTimePredictionOnlyAccess

`AmazonMachineLearningRealTimePredictionOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Benutzern die Erlaubnis erteilt, Echtzeit-Vorhersagen von Amazon Machine Learning anzufordern.

Verwenden dieser -Richtlinie

Sie können`AmazonMachineLearningRealTimePredictionOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. April 2015, 17:44 UTC
- Bearbeitete Zeit: 9. April 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMachineLearningRoleforRedshiftDataSourceV3

`AmazonMachineLearningRoleforRedshiftDataSourceV3`ist eine AWSverwaltete Richtlinie, die: Machine Learning die Konfiguration und Verwendung Ihrer Redshift-Cluster und S3-Staging-Standorte für Redshift-Datenquellen ermöglicht.

Verwenden dieser -Richtlinie

Sie können`AmazonMachineLearningRoleforRedshiftDataSourceV3` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 24. Juni 2020, 18:00 UTC
- Bearbeitete Zeit: 24. Juni 2020, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMacieFullAccess

`AmazonMacieFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Macie bietet.

Verwenden dieser -Richtlinie

Sie könnenAmazonMacieFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. August 2017, 14:54 UTC
- Bearbeitete Zeit: 1. Juli 2022, 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieFullAccess

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMacieHandshakeRole

`AmazonMacieHandshakeRole`ist eine AWSverwaltete Richtlinie, die: Erteilt die Erlaubnis, die serviceverknüpfte Rolle von Amazon Macie zu erstellen.

Verwenden dieser -Richtlinie

Sie können`AmazonMacieHandshakeRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 28. Juni 2018, 15:46 UTC
- Bearbeitete Zeit: 28. Juni 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMacieReadOnlyAccess

`AmazonMacieReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Macie bietet.

Verwendung dieser Richtlinie

Sie können Verbindungen `AmazonMacieReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Juni 2023, 21:50 UTC
- Bearbeitete Zeit: 15. Juni 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AmazonMacieServiceRole

`AmazonMacieServiceRole`ist eine AWSverwaltete Richtlinie, die: Macie Lesezugriff auf die Ressourcenabhängigkeiten in Ihrem Konto gewährt, um die Datenanalyse zu ermöglichen.

Verwenden dieser -Richtlinie

Sie können`AmazonMacieServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. August 2017, 14:53 UTC
- Bearbeitete Zeit: 14. August 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalRichtlinien und Umstellung auf Berechtigungen

AmazonMacieServiceRolePolicy

`AmazonMacieServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Serviceverknüpfte Rolle für Amazon Macie

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. Juni 2018, 22:17 UTC
- Bearbeitete Zeit: 19. Mai 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONRichtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonManagedBlockchainConsoleFullAccess

`AmazonManagedBlockchainConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Managed Blockchain bietet über dieAWS Management Console

Verwenden dieser Richtlinien

Sie können`AmazonManagedBlockchainConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 29. April 2019, 21:23 UTC
- Bearbeitete Zeit: 29. April 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonManagedBlockchainFullAccess

`AmazonManagedBlockchainFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Managed Blockchain bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonManagedBlockchainFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. April 2019, 21:39 UTC
- Bearbeitete Zeit: 29. April 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version ist die -verwaltete -verwaltete -verwaltete -verwaltete -verwal Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonManagedBlockchainReadOnlyAccess

`AmazonManagedBlockchainReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Managed Blockchain gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonManagedBlockchainReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Erstellungszeit: 30. April 2019, 18:17 UTC
- Bearbeitete Zeit: 30. April 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien und Umstellung auf -verwalteter

AmazonManagedBlockchainServiceRolePolicy

`AmazonManagedBlockchainServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und Ressourcen, die von Amazon Managed Blockchain verwendet oder verwaltet werden, ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die der Service die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. Januar 2020, 19:51 UTC
- Bearbeitete Zeit: 17. Januar 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS verwalteter Richtlinien

AmazonMCSFullAccess

`AmazonMCSFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Managed Apache Cassandra Service bietet

Verwenden dieser Richtlinien

Sie können`AmazonMCSFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 13:45 UTC
- Bearbeitete Zeit: 17. April 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMCSReadOnlyAccess

`AmazonMCSReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Managed Apache Cassandra Service gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonMCSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 13:46 UTC
- Bearbeitete Zeit: 17. April 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMechanicalTurkFullAccess

`AmazonMechanicalTurkFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf alle APIs in Amazon Mechanical Turk bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonMechanicalTurkFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Dezember 2015, 19:08 UTC
- Bearbeitete Zeit: 11. Dezember 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMechanicalTurkReadOnly

`AmazonMechanicalTurkReadOnly`ist eine AWSverwaltete Richtlinie, die: Zugriff auf schreibgeschützten APIs in Amazon Mechanical Turk bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonMechanicalTurkReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Dezember 2015, 19:08 UTC
- Bearbeitete Zeit: 25. September 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMemoryDBFullAccess

`AmazonMemoryDBFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon MemoryDB über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonMemoryDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Oktober 2021, 19:24 UTC
- Bearbeitete Zeit: 8. Oktober 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMemoryDBReadOnlyAccess

`AmazonMemoryDBReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon MemoryDB über dieAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonMemoryDBReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Oktober 2021, 19:27 UTC
- Bearbeitete Zeit: 8. Oktober 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMobileAnalyticsFinancialReportAccess

`AmazonMobileAnalyticsFinancialReportAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf alle Berichte einschließlich Finanzdaten für alle Anwendungsressourcen bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonMobileAnalyticsFinancialReportAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMobileAnalyticsFullAccess

`AmazonMobileAnalyticsFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alle Anwendungsressourcen bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonMobileAnalyticsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC

- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMobileAnalyticsNon-financialReportAccess

`AmazonMobileAnalyticsNon-financialReportAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf nicht finanzielle Berichte für alle Anwendungsressourcen bietet.

Verwenden dieser -Richtlinie

Sie könnenAmazonMobileAnalyticsNon-financialReportAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMobileAnalyticsWriteOnlyAccess

`AmazonMobileAnalyticsWriteOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Schreibzugriff auf Put-Ereignisdaten für alle Anwendungsressourcen bereitstellt. (Für die SDK-Integration empfohlen)

Verwenden dieser -Richtlinie

Sie können`AmazonMobileAnalyticsWriteOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:PutEvents",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMonitronFullAccess

`AmazonMonitronFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf die Verwaltung von Amazon Monitron bietet

Verwenden dieser -Richtlinie

Sie können`AmazonMonitronFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. Dezember 2020, 22:40 UTC
- Bearbeitete Zeit: 8. Juni 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMQApiFullAccess

`AmazonMQApiFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf AmazonMQ über unsere API/SDK bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonMQApiFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Dezember 2018, 20:31 UTC
- Bearbeitete Zeit: 4. November 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMQApiReadOnlyAccess

`AmazonMQApiReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Über unsere API/SDK nur Lesezugriff auf AmazonMQ ermöglicht.

Verwenden dieser -Richtlinie

Sie können`AmazonMQApiReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Dezember 2018, 20:31 UTC
- Bearbeitete Zeit: 18. Dezember 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON--Richtliniendokument

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

```
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMQFullAccess

`AmazonMQFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf AmazonMQ über die gewährtAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonMQFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. November 2017, 15:28 UTC
- Bearbeitete Zeit: 4. November 2020, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMQReadOnlyAccess

`AmazonMQReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf AmazonMQ über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonMQReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. November 2017, 15:30 UTC
- Bearbeitete Zeit: 28. November 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMQServiceRolePolicy

`AmazonMQServiceRolePolicy`ist eine [AWSverwaltete Richtlinie](), die: Service Linked Role Policy fürAWS Amazon MQ

Verwenden dieser Richtlinien Richtlinien Richtlinien Richtlinien Richtlinien

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 04. November 2020, 04. November 2020:04. November 2020:04. November 2020
- Bearbeitete Zeit: 4. November 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinien ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richt-Richtdokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen.

AmazonMSKConnectReadOnlyAccess

`AmazonMSKConnectReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon MSK Connect gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonMSKConnectReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. September 2021, 10:18 UTC
- Bearbeitete Zeit: 18. Oktober 2021, 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMSKFullAccess

`AmazonMSKFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon MSK und andere erforderliche Berechtigungen für die zugehörigen Abhängigkeiten gewährt.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMSKFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Januar 2019, 22:07 UTC
- Bearbeitete Zeit: 18. Oktober 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMSKReadOnlyAccess

`AmazonMSKReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon MSK gewährt

Verwenden dieser Richtlinie

Sie können`AmazonMSKReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Januar 2019, 22:28 UTC
- Bearbeitete Zeit: 14. Januar 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonMWAAServiceRolePolicy

`AmazonMWAAServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Die von Amazon Managed Workflows für Apache Airflow verwendete Service Linked Role.

Diese Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 24. November 2020, 14:13 UTC
- Bearbeitete Zeit: 17. November 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinie
Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

J------

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- AWSverwalteter Richtlinien

AmazonNimbleStudio-LaunchProfileWorker

`AmazonNimbleStudio-LaunchProfileWorker`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Zugriff auf Ressourcen, die die Mitarbeiter von Nimble Studio Launch Profile benötigen. Hängen Sie diese Richtlinie an EC2-Instances an, die von Nimble Studio Builder erstellt wurden.

Verwenden dieser -Richtlinie

Sie können`AmazonNimbleStudio-LaunchProfileWorker` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. April 2021, 04:47 UTC
- Bearbeitete Zeit: 28. April 2021, 04:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonNimbleStudio-StudioAdmin

`AmazonNimbleStudio-StudioAdmin`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Zugriff auf Amazon Nimble Studio-Ressourcen, die mit dem Studio-Administrator verknüpft sind, und auf zugehörige Studio-Ressourcen in anderen Diensten. Ordnen Sie diese Richtlinie der Administratorrolle zu, die Ihrem Studio zugeordnet ist.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonNimbleStudio-StudioAdmin` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. April 2021, 04:47 UTC

- Bearbeitete Zeit: 22. September 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonNimbleStudio-StudioUser

`AmazonNimbleStudio-StudioUser`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Zugriff auf Amazon Nimble Studio-Ressourcen, die dem Studio-Benutzer zugeordnet sind, und auf zugehörige Studio-Ressourcen in anderen Diensten. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonNimbleStudio-StudioUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. April 2021, 04:48 UTC
- Bearbeitete Zeit: 22. September 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOmicsFullAccess

`AmazonOmicsFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Omics und andere erforderliche Funktionen bietetAWS-Services. Diese Richtlinie ermöglicht es dem Benutzer, RAM-Share-Einladungen zum Zugriff auf Ressourcen außerhalb des Benutzers einzusehen und anzunehmenAWS-Konto.

Verwenden dieser Richtlinien

Sie können`AmazonOmicsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Februar 2023, 00:59 UTC
- Bearbeitete Zeit: 24. Februar 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version ist die -verwaltete -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für

den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonOmicsReadOnlyAccess

`AmazonOmicsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Omics gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonOmicsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2022, 04:17 UTC
- Bearbeitete Zeit: 29. November 2022, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:Get*",
        "omics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonOneEnterpriseFullAccess

`AmazonOneEnterpriseFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Administratorberechtigungen, die den Zugriff auf alle Ressourcen und Abläufe von Amazon One Enterprise ermöglichen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOneEnterpriseFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 04:58 UTC
- Bearbeitete Zeit: 28. November 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOneEnterpriseInstallerAccess

`AmazonOneEnterpriseInstallerAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt eingeschränkte Lese- und Schreibberechtigungen, die die Installation und Aktivierung von Geräten ermöglichen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOneEnterpriseInstallerAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 05:00 UTC
- Bearbeitete Zeit: 28. November 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOneEnterpriseReadOnlyAccess

`AmazonOneEnterpriseReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt allen Amazon One Enterprise-Ressourcen und -Vorgängen nur Leseberechtigungen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOneEnterpriseReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 04:59 UTC
- Bearbeitete Zeit: 28. November 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchDashboardsServiceRolePolicy

`AmazonOpenSearchDashboardsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Amazon OpenSearch Dashboards Service ermöglicht, um auf andere AWS Dienste zuzugreifen, z. B. in CloudWatch Ihrem Namen

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. Dezember 2023, 19:38 UTC
- Bearbeitete Zeit: 22. Dezember 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchIngestionFullAccess

`AmazonOpenSearchIngestionFullAccess`ist eine AWSverwaltete Richtlinie, die: AmazonOpenSearch Ingestion den Zugriff auf andereAWS Dienste in Ihrem Namen ermöglicht.

Verwenden von -Richtlinie

Sie können`AmazonOpenSearchIngestionFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. April 2023, 18:11 UTC
- Bearbeitete Zeit: 26. April 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

-JAM-Richtlinie

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AmazonOpenSearchIngestionReadOnlyAccess

`AmazonOpenSearchIngestionReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf den AmazonOpenSearch Ingestion Service gewährt

Verwenden dieser -verwaltete -Richtlinie

Sie können`AmazonOpenSearchIngestionReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. April 2023, 18:09 UTC
- Bearbeitete Zeit: 26. April 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-JSON-Dokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
```

```
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit -verwalteteAWS -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete

AmazonOpenSearchIngestionServiceRolePolicy

`AmazonOpenSearchIngestionServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon OpenSearch Ingestion Service den Zugriff auf andereAWS Dienste in Ihrem Namen ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. November 2022, 16:49 UTC
- Bearbeitete Zeit: 18. November 2022, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonOpenSearchServerlessServiceRolePolicy

`AmazonOpenSearchServerlessServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon OpenSearch Serverless den Zugriff auf andereAWS Dienste wie CloudWatch APIs in Ihrem Namen ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 24. November 2022, 19:50 UTC
- Bearbeitete Zeit: 24. November 2022, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonOpenSearchServiceCognitoAccess

`AmazonOpenSearchServiceCognitoAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf den Amazon Cognito Cognito-Konfigurationsservice bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonOpenSearchServiceCognitoAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. September 2021, 06:31 UTC

- Bearbeitete Zeit: 20. Dezember 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonOpenSearchServiceFullAccess

`AmazonOpenSearchServiceFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den Amazon OpenSearch Service-Konfigurationsservice bietet.

Verwenden dieser Richtlinien

Sie können`AmazonOpenSearchServiceFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. September 2021, 05:33 UTC

- Bearbeitete Zeit: 8. September 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonOpenSearchServiceReadOnlyAccess

`AmazonOpenSearchServiceReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf den Amazon OpenSearch Service-Konfigurationsservice gewährt.

Verwenden dieser Richtlinie

Sie könnenAmazonOpenSearchServiceReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. September 2021, 05:38 UTC
- Bearbeitete Zeit: 8. September 2021, 05:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonOpenSearchServiceRolePolicy

`AmazonOpenSearchServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon OpenSearch Service den Zugriff auf andere AWS Dienste wie EC2 Networking APIs in Ihrem Namen ermöglicht.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. August 2021, 09:27 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPersonalizeFullAccess

`AmazonPersonalizeFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Personalize über dasAWS Management Console und SDK bietet. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, CloudWatch).

Verwenden dieser Richtlinien

Sie können`AmazonPersonalizeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 4. Dezember 2018, 22:24 UTC
- Bearbeitete Zeit: 30. Mai 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonPollyFullAccess

`AmazonPollyFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den Service und die Ressourcen von Amazon Polly gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonPollyFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. November 2016, 18:59 UTC
- Bearbeitete Zeit: 30. November 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -verwaltete -verwaltete -verwaltete Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonPollyReadOnlyAccess

`AmazonPollyReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Polly Polly-Ressourcen gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonPollyReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. November 2016, 18:59 UTC
- Bearbeitete Zeit: 17. Juli 2018, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonPrometheusConsoleFullAccess

`AmazonPrometheusConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Managed Prometheus-Ressourcen in derAWS Konsole gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonPrometheusConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Dezember 2020, 18:11 UTC
- Bearbeitete Zeit: 24. Oktober 2022, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AmazonPrometheusFullAccess

`AmazonPrometheusFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf AWS verwaltete Prometheus-Ressourcen gewährt

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonPrometheusFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 18:10 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusQueryAccess

`AmazonPrometheusQueryAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf ausgeführte Abfragen fürAWS verwaltete Prometheus-Ressourcen gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonPrometheusQueryAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Dezember 2020, 01:02 UTC
- Bearbeitete Zeit: 19. Dezember 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonPrometheusRemoteWriteAccess

`AmazonPrometheusRemoteWriteAccess`ist eine AWSverwaltete Richtlinie, die: Nur Schreibzugriff aufAWS verwaltete Prometheus-Workspaces gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonPrometheusRemoteWriteAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Dezember 2020, 01:04 UTC
- Bearbeitete Zeit: 19. Dezember 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonPrometheusScraperServiceRolePolicy

`AmazonPrometheusScraperServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf AWS Ressourcen gewährt, die von Amazon Managed Service für Prometheus Collector verwaltet oder verwendet werden

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2023, 14:19 UTC
- Bearbeitete Zeit: 26. November 2023, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:*:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "ENIUpdating",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "EKSAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:*:eks:*:*:cluster/*"
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:*:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQFullAccess

`AmazonQFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff bietet, um Interaktionen mit Amazon Q zu ermöglichen

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonQFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 16:00 Uhr UTC
- Bearbeitete Zeit: 28. November 2023, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQLDBConsoleFullAccess

`AmazonQLDBConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon QLDB über die bietetAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonQLDBConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. September 2019, 18:24 UTC
- Bearbeitete Zeit: 4. November 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Richtlinien

AmazonQLDBFullAccess

`AmazonQLDBFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon QLDB über die Service-API bietet.

Verwenden dieser Richtlinien

Sie könnenAmazonQLDBFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. September 2019, 18:23 UTC
- Bearbeitete Zeit: 4. November 2022, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBFullAccess

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonQLDBReadOnly

`AmazonQLDBReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon QLDB bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonQLDBReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. September 2019, 18:19 UTC
- Bearbeitete Zeit: 2. Juli 2021, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRDSBetaServiceRolePolicy

`AmazonRDSBetaServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es Amazon RDS ermöglicht,AWS Ressourcen in Ihrem Namen zu verwalten.

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen angehängt.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 2. Mai 2018, 19:41 UTC
- Bearbeitete Zeit: 14. Dezember 2022, 18:33 UTC

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

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
```

```
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS verwalteter Richtlinien

AmazonRDSCustomInstanceProfileRolePolicy

`AmazonRDSCustomInstanceProfileRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Ermöglicht Amazon RDS Custom, verschiedene Automatisierungsaktionen und Datenbankverwaltungsaufgaben über ein EC2-Instance-Profil auszuführen.

Verwenden dieser Richtlinie

Sie können `AmazonRDSCustomInstanceProfileRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 27. Februar 2024, 17:42 UTC
- Bearbeitungszeit: 27. Februar 2024, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonRDSCustomPreviewServiceRolePolicy

`AmazonRDSCustomPreviewServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Rollenrichtlinie für Amazon RDS Custom Preview Service

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Oktober 2021, 21:44 UTC

- Bearbeitete Zeit: 20. September 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSCustomServiceRolePolicy

`AmazonRDSCustomServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon RDS Custom ermöglicht, AWS Ressourcen in Ihrem Namen zu verwalten.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Oktober 2021, 21:39 UTC
- Bearbeitete Zeit: 20. September 2023, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
```

```
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSDataFullAccess

`AmazonRDSDataFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die Verwendung der RDS-Daten-APIs, der Secret Store-APIs für RDS-Datenbankanmeldeinformationen und der DB-Konsolen-Abfrageverwaltungs-APIs zur Ausführung von SQL-Anweisungen auf Aurora Serverless-Clustern in derAWS-Konto.

Verwenden dieser -Richtlinie

Sie können`AmazonRDSDataFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. November 2018 21:29 UTC
- Bearbeitete Zeit: 20. November 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRDSDirectoryServiceAccess

`AmazonRDSDirectoryServiceAccess`ist eine AWSverwaltete Richtlinie, die: RDS den Zugriff auf Directory Service Managed AD im Namen des Kunden für domänengebundene SQL Server-DB-Instances ermöglicht.

Verwenden dieser Richtlinie

Sie könnenAmazonRDSDirectoryServiceAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 26. Februar 2016, 02:02 UTC
- Bearbeitete Zeit: 15. Mai 2019, 16:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRDSEnhancedMonitoringRole

`AmazonRDSEnhancedMonitoringRole`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Cloudwatch für RDS Enhanced Monitoring bietet

Verwenden dieser Richtlinie

Sie können`AmazonRDSEnhancedMonitoringRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 11. November 2015, 19:58 UTC
- Bearbeitete Zeit: 11. November 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRDSFullAccess

`AmazonRDSFullAccess`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff auf Amazon RDS überAWS Management Console.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonRDSFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie
- Zeitpunkt der Erstellung: 06. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit:17. August 2023, 23:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Version der Richtlinie

Version der Richtlinie: v14(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonRDSPerformanceInsightsFullAccess

`AmazonRDSPerformanceInsightsFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf RDS Performance Insights bietet über AWS Management Console

Mit dieser Richtlinie

Sie können Verbindungen `AmazonRDSPerformanceInsightsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. August 2023, 23:41 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSPerformanceInsightsReadOnly

`AmazonRDSPerformanceInsightsReadOnly`ist eine AWSverwaltete Richtlinie, die: Schreibgeschützte Richtlinie für RDS Performance Insights

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSPerformanceInsightsReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. April 2022, 00:02 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSPreviewServiceRolePolicy

`AmazonRDSPreviewServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Rollenrichtlinie für Amazon RDS Preview Service

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 31. Mai 2018, 18:02 Uhr UTC
- Bearbeitete Zeit: 4. Oktober 2023, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSReadOnlyAccess

`AmazonRDSReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon RDS über dieAWS Management Console.

Verwenden dieser -verwaltete Richtlinien

Sie können`AmazonRDSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 14. April 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRDSServiceRolePolicy

`AmazonRDSServiceRolePolicy` ist eine -AWSverwaltete Richtlinie, die: Ermöglicht Amazon RDS, -AWSRessourcen in Ihrem Namen zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 08. Januar 2018, 18:17 UTC
- Bearbeitungszeit: 19. Januar 2024, 15:10 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonRedshiftAllCommandsFullAccess

`AmazonRedshiftAllCommandsFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie beinhaltet Berechtigungen zum Ausführen von SQL-Befehlen zum Kopieren, Laden, Entladen, Abfragen und Analysieren von Daten auf Amazon Redshift. Die Richtlinie gewährt auch Berechtigungen zum Ausführen von ausgewählten Anweisungen für verwandte Dienstleistungen wie Amazon S3, Amazon CloudWatch Logs SageMaker, Amazon oderAWS Glue.

Verwenden dieser Richtlinie

Sie können`AmazonRedshiftAllCommandsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. November 2021, 00:48 UTC
- Bearbeitete Zeit: 25. November 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONSONSONSON-Richtlinie

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRedshiftDataFullAccess

`AmazonRedshiftDataFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie vollständigen Zugriff auf die Amazon-Redshift-Data-APIs bietet. Diese Richtlinie gewährt außerdem vollständigen Zugriff auf andere erforderliche Dienste.

Verwenden dieser Richtlinie

Sie können`AmazonRedshiftDataFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. September 2020, 19:23 UTC
- Bearbeitete Zeit: 7. April 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Beginnen Sie mitAWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Berechtigungen

AmazonRedshiftFullAccess

`AmazonRedshiftFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Redshift über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonRedshiftFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 7. Juli 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRedshiftQueryEditor

`AmazonRedshiftQueryEditor`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf den Amazon Redshift Query Editor und auf gespeicherte Abfragen über den bietetAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonRedshiftQueryEditor` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. Oktober 2018, 22:50 UTC
- Bearbeitete Zeit: 16. Februar 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AmazonRedshiftQueryEditorV2FullAccess

`AmazonRedshiftQueryEditorV2FullAccess` ist eine -AWS verwaltete Richtlinie, die: Gewährt vollen Zugriff auf die Vorgänge und Ressourcen des Amazon-Redshift-Abfrage-Editors V2. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon-Redshift-Cluster, zum Lesen von Schlüsseln und Aliassen in AWS KMS und zum Verwalten der Secrets des Abfrage-Editors V2 in AWS Secrets Manager.

Verwenden dieser Richtlinie

Sie können `AmazonRedshiftQueryEditorV2FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:06 UTC
- Bearbeitungszeit: 21. Februar 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRedshiftQueryEditorV2NoSharing

`AmazonRedshiftQueryEditorV2NoSharing` ist eine von AWS verwaltete Richtlinie, die: Erteilt die Möglichkeit, mit dem Amazon Redshift Query Editor V2 zu arbeiten, ohne Ressourcen gemeinsam zu nutzen. Der gewährte Prinzipal kann nur seine eigenen Ressourcen lesen, aktualisieren und löschen, aber nicht freigeben. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon-Redshift-Cluster und zum Verwalten der Abfrage-Editor-V2-Secrets des Prinzipals in AWS Secrets Manager.

Verwenden dieser Richtlinie

Sie können `AmazonRedshiftQueryEditorV2NoSharing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:18 UTC
- Bearbeitungszeit: 21. Februar 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Richtlinienversion

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRedshiftQueryEditorV2ReadSharing

`AmazonRedshiftQueryEditorV2ReadSharing` ist eine -AWS verwaltete Richtlinie, die: Erteilt die Möglichkeit, mit dem Amazon Redshift Query Editor V2 mit eingeschränkter Freigabe von Ressourcen zu arbeiten. Der gewährte Prinzipal kann seine eigenen Ressourcen lesen, schreiben und freigeben. Der erteilte Prinzipal kann die Ressourcen lesen, die mit seinem Team geteilt wurden,

aber nicht aktualisieren. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon-Redshift-Cluster und zum Verwalten der Abfrage-Editor-V2-Secrets des Prinzipals in AWS Secrets Manager.

Verwenden dieser Richtlinie

Sie können `AmazonRedshiftQueryEditorV2ReadSharing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:22 UTC
- Bearbeitungszeit: 21. Februar 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Richtlinienversion

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRedshiftQueryEditorV2ReadWriteSharing

`AmazonRedshiftQueryEditorV2ReadWriteSharing` ist eine von AWS verwaltete Richtlinie, die: Erteilt die Möglichkeit, mit dem Amazon Redshift Query Editor V2 mit der Freigabe von Ressourcen zu arbeiten. Der gewährte Prinzipal kann seine eigenen Ressourcen lesen, schreiben und freigeben. Der Prinzipal mit den entsprechenden Berechtigungen kann die mit seinem Team geteilten Ressourcen lesen und bearbeiten. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon-Redshift-Cluster und zum Verwalten der Abfrage-Editor-V2-Secrets des Prinzipals in AWS Secrets Manager.

Verwenden dieser Richtlinie

Sie können `AmazonRedshiftQueryEditorV2ReadWriteSharing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:25 UTC
- Bearbeitungszeit: 21. Februar 2024, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Richtlinienversion

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRedshiftReadOnlyAccess

`AmazonRedshiftReadOnlyAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf Amazon Redshift über die AWS Management Console.

Verwenden dieser Richtlinie

Sie können `AmazonRedshiftReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. Februar 2015, 18:40 UTC
- Bearbeitungszeit: 08. Februar 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonRedshiftServiceLinkedRolePolicy

`AmazonRedshiftServiceLinkedRolePolicy` ist eine -AWS verwaltete Richtlinie, die: Ermöglicht Amazon Redshift, - AWS Services in Ihrem Namen aufzurufen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 18. September 2017, 19:19 UTC
- Bearbeitungszeit: 15. März 2024, 20:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Richtlinienversion

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonRekognitionCustomLabelsFullAccess

`AmazonRekognitionCustomLabelsFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie spezifiziert die Rekognition- und s3-Berechtigungen, die für die Amazon Rekognition Custom Labels-Funktion erforderlich sind.

Verwenden dieser Richtlinie

Sie können`AmazonRekognitionCustomLabelsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Januar 2020, 19:18 UTC

- Bearbeitete Zeit: 16. August 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRekognitionFullAccess

`AmazonRekognitionFullAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf alle Amazon Rekognition Rekognition-APIs

Verwenden dieser -Richtlinie

Sie können`AmazonRekognitionFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. November 2016, 14:40 UTC
- Bearbeitete Zeit: 30. November 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AmazonRekognitionReadOnlyAccess

`AmazonRekognitionReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf alle Read Rekognition APIs

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRekognitionReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 14:58 Uhr UTC
- Bearbeitete Zeit: 8. November 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionServiceRole

`AmazonRekognitionServiceRole`ist eine AWSverwaltete Richtlinie, die: Rekognition ermöglicht,AWS Dienste in Ihrem Namen anzurufen.

Verwenden dieser -Richtlinie

Sie können`AmazonRekognitionServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 29. November 2017, 16:52 UTC
- Bearbeitete Zeit: 29. November 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53AutoNamingFullAccess

`AmazonRoute53AutoNamingFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alle automatischen Benennungsaktionen von Route 53 bietet.

Verwenden dieser

Sie können`AmazonRoute53AutoNamingFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Januar 2018, 18:40 UTC
- Bearbeitete Zeit: 18. Januar 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AmazonRoute53AutoNamingReadOnlyAccess

`AmazonRoute53AutoNamingReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf alle automatischen Benennungsaktionen von Route 53 bietet.

Verwenden dieser Richtlinie

Sie können`AmazonRoute53AutoNamingReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Januar 2018, 03:02 UTC
- Bearbeitete Zeit: 18. Januar 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53AutoNamingRegistrantAccess

`AmazonRoute53AutoNamingRegistrantAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Registrantenebene auf Route 53 53-Aktionen zur automatischen Benennung gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonRoute53AutoNamingRegistrantAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 12. März 2018, 22:33 UTC
- Bearbeitete Zeit: 12. März 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53DomainsFullAccess

`AmazonRoute53DomainsFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf alle Aktionen von Route53 Domains und Create Hosted Zone bietet, um die Erstellung von Hosting-Zonen im Rahmen von Domainregistrierungen zu ermöglichen.

Verwenden dieser -Richtlinie

Sie können`AmazonRoute53DomainsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53DomainsReadOnlyAccess

`AmazonRoute53DomainsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Liste und Aktionen der Route53-Domänen bietet.

Verwenden dieser Richtlinie

Sie können`AmazonRoute53DomainsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsverwaltete Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung mit den geringsten Berechtigungen

AmazonRoute53FullAccess

`AmazonRoute53FullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alle Amazon Route 53 über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonRoute53FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 20. Dezember 2018, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53ReadOnlyAccess

`AmazonRoute53ReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf alle Amazon Route 53 über dieAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonRoute53ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 15. November 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53RecoveryClusterFullAccess

`AmazonRoute53RecoveryClusterFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den Amazon Route 53 Recovery Cluster bietet

Verwenden dieser -Richtlinie

Sie können`AmazonRoute53RecoveryClusterFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. August 2021, 18:37 UTC
- Bearbeitete Zeit: 18. August 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53RecoveryClusterReadOnlyAccess

`AmazonRoute53RecoveryClusterReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf den Amazon Route 53 Recovery Cluster bietet

Verwenden dieser Richtlinien

Sie können`AmazonRoute53RecoveryClusterReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. August 2021, 17:36 UTC
- Bearbeitete Zeit: 1. April 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53RecoveryControlConfigFullAccess

`AmazonRoute53RecoveryControlConfigFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Route 53 Recovery Control Config bietet

Verwenden dieser -verwaltete Richtlinie

Sie können`AmazonRoute53RecoveryControlConfigFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. August 2021, 17:48 UTC

- Bearbeitete Zeit: 18. August 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion definiert die Berechtigungen für die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53RecoveryControlConfigReadOnlyAccess

`AmazonRoute53RecoveryControlConfigReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf Amazon Route 53 Recovery Control Config bietet

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53RecoveryControlConfigReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 18:01 UTC
- Bearbeitete Zeit: 18. Oktober 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryReadinessFullAccess

`AmazonRoute53RecoveryReadinessFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Route 53 Recovery Readiness bietet

Verwenden dieser -Richtlinie

Sie können`AmazonRoute53RecoveryReadinessFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. August 2021, 16:45 UTC
- Bearbeitete Zeit: 18. August 2021, 16:45 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53RecoveryReadinessReadOnlyAccess

`AmazonRoute53RecoveryReadinessReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Route 53 Recovery Readiness gewährt

Verwenden dieser -Richtlinie

Sie könnenAmazonRoute53RecoveryReadinessReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. August 2021, 18:11 UTC
- Bearbeitete Zeit: 9. November 2021, 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53ResolverFullAccess

`AmazonRoute53ResolverFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollständige Zugriffsrichtlinie für Route 53 Resolver

Verwenden dieser -Richtlinie

Sie können`AmazonRoute53ResolverFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. Mai 2019, 18:10 UTC
- Bearbeitete Zeit: 17. Juli 2020, 19:03 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonRoute53ResolverReadOnlyAccess

`AmazonRoute53ResolverReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Read-Only-Richtlinie für Route 53 Resolver

Verwenden dieser -Richtlinie

Sie können`AmazonRoute53ResolverReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. Mai 2019, 18:11 UTC
- Bearbeitete Zeit: 27. September 2019, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonS3FullAccess

`AmazonS3FullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alle Buckets über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonS3FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 27. September 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonS3ObjectLambdaExecutionRolePolicy

`AmazonS3ObjectLambdaExecutionRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Lambda-Funktionen Berechtigungen für die Interaktion mit Amazon S3 Object Lambda bereitstellt. Erteilt außerdem Lambda-Berechtigungen zum Schreiben in CloudWatch Logs.

Verwenden dieser Richtlinie

Sie könnenAmazonS3ObjectLambdaExecutionRolePolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 18. August 2021, 10:07 UTC
- Bearbeitete Zeit: 18. August 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonS3OutpostsFullAccess

`AmazonS3OutpostsFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon S3 auf Outposts über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonS3OutpostsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. Oktober 2020, 17:26 UTC
- Bearbeitete Zeit: 2. Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonS3OutpostsReadOnlyAccess

`AmazonS3OutpostsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon S3 auf Outposts über dieAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AmazonS3OutpostsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. Oktober 2020, 18:55 UTC
- Bearbeitete Zeit: 2. Oktober 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonS3ReadOnlyAccess

`AmazonS3ReadOnlyAccess`ist einAWSverwaltete Richtliniedas: Bietet schreibgeschützten Zugriff auf alle Buckets überAWS Management Console.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonS3ReadOnlyAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie
- Zeitpunkt der Erstellung: 06. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit:10. August 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie: v3(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Dienstorollenrichtlinie, die vomAWS-Service Katalogdienst zur Bereitstellung von Produkten aus dem SageMaker Amazon-Produktportfolio verwendet wird. Erteilt Berechtigungen für eine Reihe verwandter Dienste CodePipeline CodeBuild CodeCommit, darunter, CloudFormation, Glue usw.

Verwenden dieser -Richtlinie

Sie können`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2020, 18:48 UTC
- Bearbeitete Zeit: 2. August 2022, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Richtlinie definiert die Richtlinien und Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerCanvasAIServicesAccess

`AmazonSageMakerCanvasAIServicesAccess`ist eine AWSverwaltete Richtlinie, die: Amazon SageMaker Canvas die Erlaubnis erteilt, KI-Services zur Unterstützung einsatzbereiter KI-Lösungen zu nutzen. Diese Richtlinie wird weitere Mutationsberechtigungen für Dienste hinzufügen, sobald Amazon SageMaker Canvas Unterstützung anbietet.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonSageMakerCanvasAIServicesAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. März 2023, 22:36 UTC
- Bearbeitete Zeit: 29. November 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasBedrockAccess

`AmazonSageMakerCanvasBedrockAccess` ist eine von AWS verwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen zur Verwendung von Amazon Bedrock in SageMaker Canvas, indem sie Zugriff auf nachgelagerte Services wie S3 gewährt.

Verwenden dieser Richtlinie

Sie können `AmazonSageMakerCanvasBedrockAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 02. Februar 2024, 18:37 UTC
- Bearbeitungszeit: 02. Februar 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasDataPrepFullAccess

`AmazonSageMakerCanvasDataPrepFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf SageMaker Amazon-Ressourcen und -Operationen für die Datenaufbereitung in Canvas bietet. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue EventBridge, Secrets Manager). Diese Richtlinie sollte der Ausführungsrolle SageMaker Amazon-Domain/Benutzerprofil zugeordnet werden.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonSageMakerCanvasDataPrepFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2023, 22:56 UTC
- Bearbeitete Zeit: 8. Dezember 2023, 02:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasDirectDeployAccess

`AmazonSageMakerCanvasDirectDeployAccess`ist eine AWSverwaltete Richtlinie, die: Amazon SageMaker Canvas ermöglicht, Endpunktdetails für Endgeräte zu erstellen, zu verwalten und anzuzeigen, die über Canvas erstellt wurden. Ermöglicht Amazon SageMaker Canvas das Abrufen von Messdaten zum Aufrufen von Endpunkten. CloudWatch

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonSageMakerCanvasDirectDeployAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Oktober 2023, 18:11 UTC
- Bearbeitete Zeit: 6. Oktober 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasForecastAccess

`AmazonSageMakerCanvasForecastAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen, die üblicherweise für die Verwendung von SageMaker Canvas mit Amazon Forecast erforderlich sind.

Verwenden dieser Richtlinie

Sie können`AmazonSageMakerCanvasForecastAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 24. August 2022, 20:04 UTC
- Bearbeitete Zeit: 24. August 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerCanvasFullAccess

`AmazonSageMakerCanvasFullAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf Amazon SageMaker Canvas-Ressourcen und -Operationen. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Services (z. B. S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager und Forecast). Diese Richtlinie sollte an die Ausführungsrolle von Amazon SageMaker Domain/User Profile angehängt werden.

Verwenden dieser Richtlinie

Sie können `AmazonSageMakerCanvasFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 9. September 2022, 00:44 UTC
- Bearbeitungszeit: 24. Januar 2024, 22:01 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Richtlinienversion

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonSageMakerClusterInstanceRolePolicy

`AmazonSageMakerClusterInstanceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen, die üblicherweise für die Verwendung von Amazon SageMaker Cluster benötigt werden.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerClusterInstanceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 15:11 UTC
- Bearbeitete Zeit: 29. November 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCoreServiceRolePolicy

`AmazonSageMakerCoreServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Verwaltete Richtlinie für Service Linked Role für Amazon SageMaker Core Services

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. Dezember 2020, 21:40 UTC
- Bearbeitete Zeit: 21. Dezember 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie definiert die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienlinienlinien

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten

AmazonSageMakerEdgeDeviceFleetPolicy

`AmazonSageMakerEdgeDeviceFleetPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen bereitstellt, die SageMaker Edge benötigt, um eine Geräteflotte für den Kunden mithilfe der Standard-Cloud-Verbindung zu erstellen und zu verwalten.

Verwenden dieser -Richtlinie

Sie könnenAmazonSageMakerEdgeDeviceFleetPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 8. Dezember 2020, 16:17 UTC
- Bearbeitete Zeit: 8. Dezember 2020, 16:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerFeatureStoreAccess

`AmazonSageMakerFeatureStoreAccess`ist eine AWSverwaltete Richtlinie, die: Berechtigungen bereitstellt, die erforderlich sind, um den Offline-Shop für eine SageMaker FeatureStore Amazon-Feature-Gruppe zu aktivieren.

Verwenden dieser -verwaltete Richtlinien

Sie können`AmazonSageMakerFeatureStoreAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2020, 16:24 UTC
- Bearbeitete Zeit: 5. Dezember 2022, 14:19 UTC

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

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerFullAccess

`AmazonSageMakerFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon SageMaker über das SDK AWS Management Console und bietet. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, ECR, CloudWatch Logs).

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AmazonSageMakerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 13:07 UTC
- Bearbeitete Zeit: 30. November 2023, 13:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Version der Richtlinie

Richtlinienversion: v25 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
```

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

```
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
```

```
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
```

```
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
```

```
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
```

```
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
```

```
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
```

```
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
```

```
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
```

```
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerGeospatialExecutionRole

`AmazonSageMakerGeospatialExecutionRole`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie den Zugriff auf Dienste ermöglicht, die üblicherweise für die Nutzung vonSageMaker Geodaten benötigt werden.

Verwenden dieser Richtlinie

Sie können`AmazonSageMakerGeospatialExecutionRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 30. November 2022, 10:08 UTC
- Bearbeitete Zeit: 10. Mai 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen und -verwaltete Berechtigungen mit
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen und Umstellung

AmazonSageMakerGeospatialFullAccess

`AmazonSageMakerGeospatialFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen, die den vollen Zugriff auf Amazon SageMaker Geospatial über dasAWS Management Console und SDK ermöglichen.

Verwenden dieser Richtlinie

Sie könnenAmazonSageMakerGeospatialFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 30. November 2022
- Bearbeitete Zeit: 30. November 2022, 10:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Funktion für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von -AM-Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerGroundTruthExecution

`AmazonSageMakerGroundTruthExecution`ist eine AWSverwaltete Richtlinie, die: Zugriff aufAWS Dienste bietet, die für die Ausführung des SageMaker GroundTruth Labeling-Jobs erforderlich sind

Verwenden dieser Richtlinie

Sie können`AmazonSageMakerGroundTruthExecution` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Juli 2020, 19:30 UTC
- Bearbeitete Zeit: 29. April 2022, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerMechanicalTurkAccess

`AmazonSageMakerMechanicalTurkAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Erstellung von Amazon Augmented FlowDefinition AI-Ressourcen für jedes Workteam bietet.

Verwenden dieser Richtlinie

Sie könnenAmazonSageMakerMechanicalTurkAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 16:19 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerModelGovernanceUseAccess

`AmazonSageMakerModelGovernanceUseAccess`ist einAWSverwaltete Richtliniedas: DasAWSDie verwaltete Richtlinie gewährt die für die Nutzung aller Amazon-Produkte erforderlichen BerechtigungenSageMakerVerwaltungsfunktionen. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, KMS).

Verwendung dieser Richtlinie

Sie können anhängen`AmazonSageMakerModelGovernanceUseAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 30. November 2022, 08:58 Uhr UTC
- Uhrzeit der Bearbeitung:17. Juli 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Version der Richtlinie

Version der Richtlinie: v2(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonSageMakerModelRegistryFullAccess

`AmazonSageMakerModelRegistryFullAccess`ist eine AWSverwaltete Richtlinie, die: Dies ist eine neue verwaltete Richtlinie für Model Registry in Sagemaker. Diese Richtlinie ist eine eigenständige Richtlinie, die an die Benutzerrolle angehängt werden kann, um auf Funktionen im Zusammenhang mit Model Registry in Sagemaker zuzugreifen.

Verwenden dieser -Richtlinie

Sie können`AmazonSageMakerModelRegistryFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. April 2023, 05:20 UTC
- Bearbeitete Zeit: 13. April 2023, 05:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die Berechtigungen für die -Funktion für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerNotebooksServiceRolePolicy

`AmazonSageMakerNotebooksServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Verwaltete Richtlinie für Service Linked Role für Amazon SageMaker Notebooks

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. Oktober 2019, 20:27 UTC
- Bearbeitete Zeit: 9. März 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`ist einAWSverwaltete Richtliniedas: Servicerollenrichtlinie, die von derAWSApiGateway innerhalb

derAWS ServiceCatalogbereitgestellte Produkte von AmazonSageMakerPortfolio von Produkten. Erteilt Berechtigungen für eine Reihe verwandter Dienste, darunter Lambda und andere.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Servicerollen
- Entstehungszeit: 01. August 2023, 15:06 Uhr UTC
- Uhrzeit der Bearbeitung:01. August 2023, 15:06 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eineAWSressource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`ist einAWSverwaltete Richtliniedas: Servicerollenrichtlinie, die von derAWS CloudFormationinnerhalb derAWS ServiceCatalogbereitgestellte Produkte von AmazonSageMakerPortfolio von Produkten. Erteilt Berechtigungen für eine Teilmenge verwandter Dienste, darunter Lambda, ApiGateway und andere.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePoli` Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Servicerollen
- Zeit der Erstellung: 01. August 2023, 15:06 Uhr UTC
- Uhrzeit der Bearbeitung:01. August 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine`AWS`Ressource,`AWS`überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`ist einAWSverwaltete Richtliniedas: Servicerollenrichtlinie, die von derAWSLambda innerhalb derAWS ServiceCatalogbereitgestellte Produkte von AmazonSageMakerPortfolio von Produkten. Erteilt Berechtigungen für eine Reihe verwandter Dienste, darunter Secrets Manager und andere.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Servicerollen
- Entstehungszeit: 01. August 2023, 15:05 Uhr UTC
- Uhrzeit der Bearbeitung:01. August 2023, 15:05 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf

eineAWSressource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonSageMakerPipelinesIntegrations

`AmazonSageMakerPipelinesIntegrations`ist eine AWSverwaltete Richtlinie, die: Diese Amazon Managed Policy gewährt Berechtigungen, die üblicherweise für die Verwendung mit Callback-Schritten und Lambda-Schritten in SageMaker Model Building-Pipelines benötigt werden. Es wird dem hinzugefügt AmazonSageMaker -ExecutionRole , das bei der Einrichtung von SageMaker

Studio erstellt werden kann. Sie kann auch an jede andere Rolle angehängt werden, die für die Erstellung oder Ausführung von Pipelines verwendet wird.

Verwenden dieser -Richtlinie

Sie könnenAmazonSageMakerPipelinesIntegrations an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. Juli 2021, 16:35 UTC
- Bearbeitete Zeit: 17. Februar 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerReadOnly

`AmazonSageMakerReadOnly`ist eine AWSverwaltete Richtlinie, die: SageMaker Über dasAWS Management Console und SDK nur Lesezugriff auf Amazon bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonSageMakerReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2017, 13:07 UTC

- Bearbeitete Zeit: 1. Dezember 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Version der Richtlinie

Version der Richtlinie:v11 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie und Umstellung auf Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Dienstorollenrichtlinie, dieAWS vom ApiGateway innerhalb des von AmazonAWS ServiceCatalog bereitgestellten SageMaker Produktportfolios verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, einschließlich CloudWatch Logs und anderen.

Verwenden dieser -Richtlinie

Sie können`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 25. März 2022, 04:25 UTC
- Bearbeitete Zeit: 25. März 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Dienstorollenrichtlinie, dieAWS CloudFormation von denAWS ServiceCatalog bereitgestellten Produkten aus dem SageMaker Amazon-Produktportfolio verwendet wird. Erteilt Genehmigungen für eine Untergruppe verwandter Dienste, darunter SageMaker auch für andere.

Verwenden dieser Richtlinie

Sie können`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 25. März 2022, 04:26 UTC
- Bearbeitete Zeit: 25. März 2022, 04:26 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Dienstorollenrichtlinie, dieAWS CodeBuild von denAWS ServiceCatalog bereitgestellten Produkten aus dem SageMaker Amazon-Produktportfolio verwendet wird. Erteilt Berechtigungen für eine Untergruppe verwandter Dienste CodePipeline, CodeBuild darunter auch für andere.

Verwenden dieser -Richtlinie

Sie können`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. März 2022, 04:27 UTC
- Bearbeitete Zeit: 25. März 2022, 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Dienstorollenrichtlinie, dieAWS CodePipeline von denAWS ServiceCatalog bereitgestellten Produkten aus dem SageMaker Amazon-Produktportfolio verwendet wird. Erteilt Berechtigungen für eine Untergruppe verwandter Dienste CodePipeline, CodeBuild darunter auch für andere.

Verwenden dieser -Richtlinie

Sie können`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 22. Februar 2022, 09:53 UTC
- Bearbeitete Zeit: 22. Februar 2022, 09:53 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Dienstorollenrichtlinie, die von denAWS CloudWatch Events innerhalb derAWS ServiceCatalog bereitgestellten Produkte aus dem SageMaker Amazon-Produktportfolio verwendet wird. Erteilt Genehmigungen für eine Untergruppe verwandter Dienste, darunter CodePipeline auch für andere.

Verwenden von dieser -verwaltete Richtlinien

Sie können`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 22. Februar 2022, 09:53 UTC
- Bearbeitete Zeit: 22. Februar 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Version ist die -verwaltete Version, die die Berechtigungen für die -verwaltete -verwaltete -verwaltete -verwaltete Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Dienstorollenrichtlinie, die vonAWS Firehose innerhalb des von AmazonAWS ServiceCatalog bereitgestellten SageMaker Produktportfolios verwendet wird. Erteilt Genehmigungen für eine Reihe verwandter Dienste, einschließlich Firehose und anderen.

Verwenden dieser Richtlinien

Sie können`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 22. Februar 2022, 09:54 UTC
- Bearbeitete Zeit: 22. Februar 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie für die Servicerolle, die von TheAWS Glue innerhalb des von

AmazonAWS ServiceCatalog bereitgestellten SageMaker Produktportfolios verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Glue, S3 und andere.

Verwenden dieser -Richtlinie

Sie könnenAmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 22. Februar 2022, 09:51 UTC
- Bearbeitete Zeit: 26. August 2022, 19:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Dienstorollenrichtlinie, die vonAWS Lambda innerhalb desAWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter ECR, S3 und andere.

Verwenden dieser -Richtlinie

Sie können`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 4. April 2022, 16:34 UTC
- Bearbeitete Zeit: 04. April 2022, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSecurityLakeAdministrator

`AmazonSecurityLakeAdministrator` ist eine -AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf Amazon Security Lake und zugehörige Services, die zur Verwaltung von Security Lake erforderlich sind.

Verwenden dieser Richtlinie

Sie können `AmazonSecurityLakeAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2023, 22:04 UTC
- Bearbeitungszeit: 23. Februar 2024, 16:01 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSecurityLakeMetastoreManager

`AmazonSecurityLakeMetastoreManager` ist eine von AWS verwaltete Richtlinie, die: Richtlinie für Amazon SecurityLake Meta Store Manager Lambda, die den Zugriff auf Cloudwatch, S3, Glue und SQS ermöglicht.

Verwenden dieser Richtlinie

Sie können `AmazonSecurityLakeMetastoreManager` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 23. Januar 2024, 15:26 UTC
- Bearbeitungszeit: 23. Januar 2024, 15:26 UTC

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

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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}"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonSecurityLakePermissionsBoundary

`AmazonSecurityLakePermissionsBoundary`ist eine AWSverwaltete Richtlinie, die: Amazon Security Lake IAM-Rollen für benutzerdefinierte Quellen von Drittanbietern erstellt, um Daten in einen Data Lake zu schreiben, und für Drittanbieter-Abonnenten, um Daten aus einem Data Lake zu nutzen, und diese Richtlinie bei der Erstellung dieser Rollen verwendet, um die Grenze ihrer Berechtigungen zu definieren.

Verwenden dieser -Richtlinie

Sie können`AmazonSecurityLakePermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2022, 14:11 UTC
- Bearbeitete Zeit: 29. November 2022, 14:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
```

```
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:sqs:arn" : [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSESFullAccess

`AmazonSESFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon SES über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonSESFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSESReadOnlyAccess

`AmazonSESReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon SES über dieAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AmazonSESReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSNSFullAccess

`AmazonSNSFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon SNS über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonSNSFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie ist die -verwaltete -Richtlinie, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSNSReadOnlyAccess

`AmazonSNSReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf Amazon SNS über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AmazonSNSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
        "sns:GetTopicAttributes",
        "sns:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSNSRole

`AmazonSNSRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Amazon SNS SNS-Servicerolle.

Verwenden dieser -Richtlinie

Sie können`AmazonSNSRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSQSFullAccess

`AmazonSQSFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon SQS über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie könnenAmazonSQSFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSQSReadOnlyAccess

`AmazonSQSReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf Amazon SQS über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können Verbindungen `AmazonSQSReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 06. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 15. Juni 2023, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSSMAutomationApproverAccess

`AmazonSSMAutomationApproverAccess`ist eine AWSverwaltete -Richtlinie, die den Zugriff ermöglicht, um Automatisierungsausführungen anzuzeigen und Genehmigungsentscheidungen an Automatisierungen zu senden, die auf Genehmigung warten

Verwenden dieser Richtlinie

Sie können`AmazonSSMAutomationApproverAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. August 2017, 23:07 UTC

- Bearbeitete Zeit: 7. August 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit den geringsten stenAWS sten sten sten sten sten sten sten sten sten sten sten sten sten sten sten sten sten sten sten sten sten sten

AmazonSSMAutomationRole

`AmazonSSMAutomationRole`ist eine AWSverwaltete Richtlinie, die: Berechtigungen für den EC2 Automation-Dienst zur Ausführung von Aktivitäten bereitstellt, die in Automatisierungsdokumenten definiert sind

Verwenden dieser -Richtlinie

Sie können`AmazonSSMAutomationRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 5. Dezember 2016, 22:09 UTC
- Bearbeitete Zeit: 24. Juli 2017, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSSMDirectoryServiceAccess

`AmazonSSMDirectoryServiceAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es SSM Agent, im Namen des Kunden auf den Directory Service zuzugreifen, um der verwalteten Instanz eine Domäne beizutreten.

Verwenden dieser -Richtlinie

Sie können`AmazonSSMDirectoryServiceAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. März 2019, 17:44 UTC
- Bearbeitete Zeit: 15. März 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSSMFullAccess

`AmazonSSMFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon SSM bietet.

Verwenden dieser Richtlinie

Sie können`AmazonSSMFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 29. Mai 2015, 17:39 UTC
- Bearbeitete Zeit: 20. November 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSSMMaintenanceWindowRole

`AmazonSSMMaintenanceWindowRole`ist eine AWSverwaltete Richtlinie, die: Die Service-Rolle, die für das EC2-Wartungsfenster verwendet werden soll

Verwenden dieser Richtlinie

Sie können`AmazonSSMMaintenanceWindowRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 1. Dezember 2016, 15:57 UTC
- Bearbeitete Zeit: 27. Juli 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete

AmazonSSMManagedEC2InstanceDefaultPolicy

`AmazonSSMManagedEC2InstanceDefaultPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie aktiviert dieAWS Systems Manager Manager-Funktionalität auf EC2-Instances.

Verwenden dieser -Richtlinie

Sie können`AmazonSSMManagedEC2InstanceDefaultPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. August 2022, 20:54 UTC
- Bearbeitete Zeit: 30. August 2022, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSSMManagedInstanceCore

`AmazonSSMManagedInstanceCore`ist eine AWSverwaltete Richtlinie, die: Die Richtlinie für Amazon EC2 Role, um die Kernfunktionen desAWS Systems Manager Manager-Service zu aktivieren.

Verwenden dieser -verwaltete

Sie können`AmazonSSMManagedInstanceCore` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. März 2019, 17:22 UTC
- Bearbeitete Zeit: 23. Mai 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSSMPatchAssociation

`AmazonSSMPatchAssociation`ist eine AWSverwaltete Richtlinie, die: Zugriff auf untergeordnete Instanzen für den Betrieb der Patch-Zuordnung gewährt.

Verwenden dieser -Richtlinie

Sie können`AmazonSSMPatchAssociation` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. Mai 2020, 16:00 UTC
- Bearbeitete Zeit: 13. Mai 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version ist die -verwaltete -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSSMReadOnlyAccess

`AmazonSSMReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon SSM bietet.

Verwenden Sie diese -Richtlinie

Sie können`AmazonSSMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. Mai 2015, 17:44 UTC
- Bearbeitete Zeit: 29. Mai 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen IAM-IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSSMServiceRolePolicy

`AmazonSSMServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff aufAWS Ressourcen gewährt, die von Amazon SSM verwaltet oder genutzt werden

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 13. November 2017, 19:20 UTC
- Bearbeitete Zeit: 14. September 2022, 19:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonSumerianFullAccess

`AmazonSumerianFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Sumerian bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonSumerianFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. April 2018, 20:14 UTC
- Bearbeitete Zeit: 24. April 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonTextractFullAccess

`AmazonTextractFullAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf alle Amazon Textract Textract-APIs

Verwenden dieser -Richtlinie

Sie können`AmazonTextractFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. November 2018, 19:07 UTC
- Bearbeitete Zeit: 28. November 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AmazonTextractServiceRole

`AmazonTextractServiceRole`ist eine AWSverwaltete Richtlinie, die: Textract erlaubt,AWS Dienste in Ihrem Namen anzurufen.

Verwenden dieser -Richtlinie

Sie können`AmazonTextractServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 28. November 2018, 19:12 UTC
- Bearbeitete Zeit: 28. November 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonTimestreamConsoleFullAccess

`AmazonTimestreamConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die Verwaltung von Amazon Timestream mit dem bietetAWS Management Console. Beachten Sie, dass diese Richtlinie auch Berechtigungen für bestimmte KMS-Operationen und Operationen zur Verwaltung Ihrer gespeicherten Abfragen gewährt. Wenn Sie vom Kunden verwaltetes

CMK verwenden, entnehmen Sie bitte der Dokumentation, welche zusätzlichen Berechtigungen erforderlich sind.

Verwenden dieser Richtlinie

Sie könnenAmazonTimestreamConsoleFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. September 2020, 21:47 UTC
- Bearbeitete Zeit: 1. Februar 2022, 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie definiert die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonTimestreamFullAccess

`AmazonTimestreamFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Timestream bietet. Beachten Sie, dass diese Richtlinie auch den Zugriff auf bestimmte KMS-Operationen gewährt. Wenn Sie vom Kunden verwaltetes CMK verwenden, entnehmen Sie bitte der Dokumentation, welche zusätzlichen Berechtigungen erforderlich sind.

Verwenden dieser -Richtlinie

Sie können`AmazonTimestreamFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. September 2020, 21:47 UTC
- Bearbeitete Zeit: 26. November 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonTimestreamInfluxDBFullAccess

`AmazonTimestreamInfluxDBFullAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet vollständigen administrativen Zugriff zum Erstellen, Aktualisieren, Löschen und Auflisten von Amazon-Timestream-InfluxDB-Instances sowie zum Erstellen und Auflisten von Parametergruppen. Weitere erforderliche Berechtigungen finden Sie in der Dokumentation.

Verwenden dieser Richtlinie

Sie können `AmazonTimestreamInfluxDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 14. März 2024, 22:53 UTC
- Bearbeitungszeit: 14. März 2024, 22:53 UTC

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

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonTimestreamInfluxDBServiceRolePolicy

`AmazonTimestreamInfluxDBServiceRolePolicy` ist eine -AWS verwaltete Richtlinie, die: Bietet vollständigen administrativen Zugriff zum Erstellen, Aktualisieren, Löschen und Auflisten von Amazon-Timestream-InfluxDB-Instances sowie zum Erstellen und Auflisten von Parametergruppen. Weitere erforderliche Berechtigungen finden Sie in der Dokumentation.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 14. März 2024, 18:53 UTC
- Bearbeitungszeit: 14. März 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonTimestreamReadOnlyAccess

`AmazonTimestreamReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Timestream gewährt. Die Richtlinie bietet auch die Erlaubnis, jede laufende Abfrage

abzubrechen. Wenn Sie vom Kunden verwaltetes CMK verwenden, entnehmen Sie bitte der Dokumentation, welche zusätzlichen Berechtigungen erforderlich sind.

Verwenden dieser -Richtlinie

Sie können`AmazonTimestreamReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. September 2020, 21:47 UTC
- Bearbeitete Zeit: 28. Februar 2023, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine`AWS` Ressource stellt,`AWS` überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonTranscribeFullAccess

`AmazonTranscribeFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den Betrieb von Amazon Transcribe bietet

Verwenden dieser -Richtlinie

Sie können`AmazonTranscribeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. April 2018, 16:06 UTC
- Bearbeitete Zeit: 4. April 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonTranscribeReadOnlyAccess

`AmazonTranscribeReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf den Nur-Lesevorgang für Amazon Transcribe bietet

Verwenden dieser -Richtlinie

Sie können`AmazonTranscribeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. April 2018, 16:05 UTC
- Bearbeitete Zeit: 4. April 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -verwaltete Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonVPCCrossAccountNetworkInterfaceOperations

`AmazonVPCCrossAccountNetworkInterfaceOperations`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Erstellung von Netzwerkschnittstellen und deren Verknüpfung mit kontoübergreifenden Ressourcen ermöglicht

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCCrossAccountNetworkInterfaceOperations` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juli 2017, 20:47 UTC
- Bearbeitete Zeit: 25. September 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCFullAccess

`AmazonVPCFullAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf Amazon VPC über die AWS Management Console.

Verwenden dieser Richtlinie

Sie können `AmazonVPCFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie

- Erstellungszeit: 06. Februar 2015, 18:41 UTC
- Bearbeitungszeit: 8. Februar 2024, 16:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Richtlinienversion

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen zum Beschreiben von AWS Ressourcen, zum Ausführen von Network Access Analyzer und zum Erstellen oder Löschen von Tags für Network Insights Access Scope und Network Insights Access Scope Analysis bereitstellt.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Juni 2023, 22:56 UTC
- Bearbeitete Zeit: 03. November 2023, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
```

```
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAccessScopeAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-access-scope/*",
        "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
```

```
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCReachabilityAnalyzerFullAccessPolicy

`AmazonVPCReachabilityAnalyzerFullAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen zum Beschreiben von AWS Ressourcen, zum Ausführen von Reachability Analyzer und zum Erstellen oder Löschen von Tags auf Network Insights Path und Network Insights Analysis bereitstellt.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCReachabilityAnalyzerFullAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Juni 2023, 20:12 UTC
- Bearbeitete Zeit: 03. November 2023, 19:37 UTC

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

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
```

```
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist der Rolle IAMRoleForReachabilityAnalyzerCrossAccountResource Access zugeordnet. Diese Rolle wird den Mitgliedskonten in einer Organisation zugewiesen, wenn das Verwaltungskonto den vertrauenswürdigen Zugriff für Reachability Analyzer ermöglicht. Es bietet Berechtigungen zum Anzeigen von Ressourcen aus Ihrem gesamten Unternehmen mithilfe der Reachability Analyzer-Konsole.

Verwenden von dieser Richtlinie mit dieser Richtlinie

Sie können`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Mai 2023, 20:38 UTC
- Bearbeitete Zeit: 1. Mai 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONRichtlinie mit -JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von IAM-AM-AM-AM-AM-AM-AM-AM-AM-AM-Richtlinie und
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AmazonVPCReadOnlyAccess

`AmazonVPCReadOnlyAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf Amazon VPC über die AWS Management Console.

Verwenden dieser Richtlinie

Sie können `AmazonVPCReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. Februar 2015, 18:41 UTC
- Bearbeitungszeit: 8. Februar 2024, 17:08 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkDocsFullAccess

`AmazonWorkDocsFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon bietet WorkDocs überAWS Management Console

Verwenden dieser Richtlinie

Sie können`AmazonWorkDocsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 16. April 2020, 23:05 UTC
- Bearbeitete Zeit: 16. April 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die Berechtigungen für die Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinie und Umstellung auf auf auf auf auf auf auf auf auf auf

AmazonWorkDocsReadOnlyAccess

`AmazonWorkDocsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon WorkDocs über dieAWS Management Console

Verwenden dieser -Richtlinie

Sie können`AmazonWorkDocsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Januar 2020, 23:49 UTC
- Bearbeitete Zeit: 8. Januar 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkMailEventsServiceRolePolicy

`AmazonWorkMailEventsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und die von Amazon WorkMail Events verwendeten oder verwalteten Ressourcen ermöglicht

Verwenden Verwenden Verwenden Verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 16. April 2019, 16:52 UTC
- Bearbeitete Zeit: 16. April 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standard Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- VerwendenAWS verwalteter Richtlinien

AmazonWorkMailFullAccess

`AmazonWorkMailFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf WorkMail Directory Service, SES, EC2 und Lesezugriff auf KMS-Metadaten bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonWorkMailFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 21. Dezember 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Version der Richtlinie

Version der Richtlinie:v10 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkMailMessageFlowFullAccess

`AmazonWorkMailMessageFlowFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die WorkMail Message Flow APIs

Verwenden dieser -Richtlinie

Sie könnenAmazonWorkMailMessageFlowFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Februar 2021, 11:08 UTC
- Bearbeitete Zeit: 11. Februar 2021, 11:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AmazonWorkMailMessageFlowReadOnlyAccess

`AmazonWorkMailMessageFlowReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf WorkMail Nachrichten für die GetRawMessageContent API

Verwenden dieser -Richtlinie

Sie können`AmazonWorkMailMessageFlowReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. Januar 2021, 12:40 UTC
- Bearbeitete Zeit: 28. Januar 2021, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workmailmessageflow:Get*"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkMailReadOnlyAccess

`AmazonWorkMailReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf WorkMail und SES gewährt.

Verwenden dieser Richtlinie

Sie können`AmazonWorkMailReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 25. Juli 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkSpacesAdmin

`AmazonWorkSpacesAdmin`ist einAWSverwaltete Richtliniedas: Bietet Zugriff auf AmazonWorkSpacesadministrative Maßnahmen überAWSSDK und CLI.

Verwendung dieser Richtlinie

Sie können anhängen`AmazonWorkSpacesAdmin`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 22. September 2015, 22:21 Uhr UTC
- Uhrzeit der Bearbeitung:03. August 2023, 23:57 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Version der Richtlinie

Version der Richtlinie: v5(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesApplicationManagerAdminAccess

`AmazonWorkSpacesApplicationManagerAdminAccess`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff für das Verpacken einer Anwendung in Amazon WorkSpaces Application Manager gewährt.

Verwenden dieser Richtlinien

Sie können`AmazonWorkSpacesApplicationManagerAdminAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 9. April 2015, 14:03 UTC
- Bearbeitete Zeit: 9. April 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkspacesPCAAccess

`AmazonWorkspacesPCAAccess`ist eine AWSverwaltete Richtlinie, die: Diese verwaltete Richtlinie bietet vollen administrativen Zugriff auf die Ressourcen der privatenAWS Zertifizierungsstelle von Certificate Manager in IhremAWS-Konto System für die zertifikatsbasierte Authentifizierung.

Verwenden dieser -Richtlinie

Sie können`AmazonWorkspacesPCAAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. November 2022, 00:25 UTC
- Bearbeitete Zeit: 8. November 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkSpacesSelfServiceAccess

`AmazonWorkSpacesSelfServiceAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf den WorkSpaces Amazon-Backend-Service bietet, um Workspace Self Service-Aktionen auszuführen

Verwenden dieser -Richtlinie

Sie können`AmazonWorkSpacesSelfServiceAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Juni 2019, 19:22 UTC
- Bearbeitete Zeit: 27. Juni 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkSpacesServiceAccess

`AmazonWorkSpacesServiceAccess`ist eine AWSverwaltete Richtlinie, die: Dem Kundenkonto den Zugriff auf denAWS WorkSpaces Dienst zum Starten eines Workspace ermöglicht.

Verwenden dieser -Richtlinie

Sie können`AmazonWorkSpacesServiceAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Juni 2019, 19:19 UTC
- Bearbeitete Zeit: 18. März 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkSpacesWebReadOnly

`AmazonWorkSpacesWebReadOnly`ist eine AWSverwaltete Richtlinie, die: Über das SDK und die CLI nur Lesezugriff auf Amazon WorkSpaces Web und seine Abhängigkeiten gewährt.AWS Management Console

Verwenden dieser Richtlinien

Sie können`AmazonWorkSpacesWebReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. November 2021, 14:20 UTC
- Bearbeitete Zeit: 2. November 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit denAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonWorkSpacesWebServiceRolePolicy

`AmazonWorkSpacesWebServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und die von Amazon WorkSpaces Web verwendeten oder verwalteten Ressourcen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 30. November 2021, 13:15 UTC
- Bearbeitete Zeit: 15. Dezember 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die StandardVersion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonZocaloFullAccess

`AmazonZocaloFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Zocalo bietet.

Verwenden dieser -Richtlinie

Sie können`AmazonZocaloFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die die Berechtigungen für die -Richtlinie für die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmazonZocaloReadOnlyAccess

`AmazonZocaloReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon Zocalo gewährt

Verwenden dieser -Richtlinie

Sie können`AmazonZocaloReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mit denAWS geringsten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AmplifyBackendDeployFullAccess

`AmplifyBackendDeployFullAccess` ist eine -AWSverwaltete Richtlinie, die: Bietet Amplify Vollzugriffsberechtigungen für die Bereitstellung von Amplify-Backend-Ressourcen (AWS AppSync, Amazon Cognito , Amazon S3 und andere verwandte Services) über das AWS Cloud Development Kit (AWS CDK)

Verwenden dieser Richtlinie

Sie können `AmplifyBackendDeployFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 06. Oktober 2023, 21:32 UTC
- Bearbeitungszeit: 02. Januar 2024, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Richtlinienversion

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

```
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ]
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableSchemaResource",
      "Effect" : "Allow",
```

```
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

APIGatewayServiceRolePolicy

`APIGatewayServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: API Gateway ermöglicht, zugehörigeAWS Ressourcen im Namen des Kunden zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 20. Oktober 2017, 17:23 UTC
- Bearbeitete Zeit: 12. Juli 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v9 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AppIntegrationsServiceLinkedRolePolicy

`AppIntegrationsServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es ermöglicht AppIntegrations , AppFlow Ressourcen zu verwalten und CloudWatch Kennzahlen in Ihrem Namen zu veröffentlichen.

Verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 30. September 2022, 19:42 UTC
- Bearbeitete Zeit: 30. September 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die -Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppIntegrations"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorEntity",
        "appflow:ListConnectorEntities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorProfiles",
        "appflow:UseConnectorProfile"
      ],
      "Resource" : "arn:aws:appflow:*:*:connector-profile/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AppIntegrationsManaged" : "true"
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:TagResource"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppIntegrationsManaged"
          ]
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- AWSErste Richtlinien

ApplicationAutoScalingForAmazonAppStreamAccess

`ApplicationAutoScalingForAmazonAppStreamAccess`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung der automatischen Skalierung von Anwendungen für Amazon AppStream

Verwenden dieser -Richtlinie

Sie können`ApplicationAutoScalingForAmazonAppStreamAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2017, 21:39 UTC
- Bearbeitete Zeit: 6. Februar 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Richtlinien Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und Ressourcen, die von der Application Discovery Service Continuous Export-Funktion verwendet oder verwaltet werden, ermöglicht.

Verwenden diese Verwenden diese

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 9. August 2018, 20:22 UTC
- Bearbeitete Zeit: 13. August 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion ist die Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
    },
```

```
    {
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
    },
    {
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS

AppRunnerNetworkingServiceRolePolicy

`AppRunnerNetworkingServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS AppRunner Networking ermöglicht, zugehörigeAWS Ressourcen in Ihrem Namen zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. Januar 2022, 21:02 UTC
- Bearbeitete Zeit: 12. Januar 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AppRunnerServiceRolePolicy

`AppRunnerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS AppRunner ermöglicht, verwandteAWS Ressourcen in Ihrem Namen zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 14. Mai 2021, 19:15 UTC
- Bearbeitete Zeit: 14. Mai 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AutoScalingConsoleFullAccess

`AutoScalingConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Auto Scaling über die bietetAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AutoScalingConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 12. Januar 2017, 19:43 UTC
- Bearbeitete Zeit: 6. Februar 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AutoScalingConsoleReadOnlyAccess

`AutoScalingConsoleReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht Lesezugriff auf Auto Scaling über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AutoScalingConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 12. Januar 2017, 19:48 UTC
- Bearbeitete Zeit: 12. Januar 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AutoScalingFullAccess

`AutoScalingFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Auto Scaling bietet.

Verwenden dieser -Richtlinie

Sie können`AutoScalingFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 12. Januar 2017, 19:31 UTC
- Bearbeitete Zeit: 6. Februar 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AutoScalingNotificationAccessRole

`AutoScalingNotificationAccessRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die AutoScaling Servicerolle Notification Access.

Verwenden dieser Richtlinie

Sie können`AutoScalingNotificationAccessRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AutoScalingReadOnlyAccess

`AutoScalingReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Schreibgeschützten Zugriff auf Auto Scaling bietet.

Verwenden dieser -Richtlinie

Sie können`AutoScalingReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 12. Januar 2017, 19:39 UTC
- Bearbeitete Zeit: 12. Januar 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie ist die -verwaltete -Richtlinie, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AutoScalingServiceRolePolicy

`AutoScalingServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Auto Scaling verwendet oder verwaltet werden

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 08. Januar 2018, 23:10 UTC
- Bearbeitungszeit: 29. Februar 2024, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWS_ConfigRole

`AWS_ConfigRole` ist eine von AWS verwaltete Richtlinie, die: Standardrichtlinie für die AWS Config-Servicerolle. Stellt Berechtigungen bereit, die AWS Config benötigt, um Änderungen an Ihren - AWS Ressourcen zu verfolgen.

Verwenden dieser Richtlinie

Sie können `AWS_ConfigRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 15. September 2020, 20:30 UTC
- Bearbeitungszeit: 22. Februar 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Richtlinienversion

Richtlinienversion: v30 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAccountActivityAccess

`AWSAccountActivityAccess`ist eine AWSverwaltete Richtlinie, die: Benutzern den Zugriff auf die Seite „Kontoaktivitäten“ ermöglicht.

Verwenden von dieser -Richtlinie

Sie könnenAWSAccountActivityAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 7. März 2023, 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountActivityAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAccountManagementFullAccess

`AWSAccountManagementFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf dieAWS Kontoverwaltung bietet.

Verwenden dieser -Richtlinie

Sie können`AWSAccountManagementFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. September 2021, 23:20 UTC
- Bearbeitete Zeit: 30. September 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die Berechtigungen für die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AWSAccountManagementReadOnlyAccess

`AWSAccountManagementReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf dieAWS Kontoverwaltung bietet

Verwenden dieser -Richtlinie

Sie könnenAWSAccountManagementReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. September 2021, 23:29 UTC
- Bearbeitete Zeit: 30. September 2021, 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die Berechtigungen für die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AWSAccountUsageReportAccess

`AWSAccountUsageReportAccess`ist eine AWSverwaltete Richtlinie, die: Benutzern den Zugriff auf die Seite mit dem Account Usage Report ermöglicht.

Verwenden dieser Richtlinie

Sie können`AWSAccountUsageReportAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf verwaltete Richtlinien

AWSAgentlessDiscoveryService

`AWSAgentlessDiscoveryService`ist eine AWSverwaltete Richtlinie, die: Ermöglicht dem Discovery Agentless Connector den Zugriff auf die Registrierung beimAWS Application Discovery Service.

Verwenden dieser -Richtlinie

Sie können`AWSAgentlessDiscoveryService` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. August 2016, 01:35 UTC
- Bearbeitete Zeit: 24. Februar 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppFabricFullAccess

`AWSAppFabricFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf den AWS AppFabric Dienst und schreibgeschützten Zugriff auf abhängige Dienste wie S3, Kinesis, KMS bietet.

Verwendung dieser Richtlinie

Sie können Verbindungen `AWSAppFabricFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 19:51 UTC
- Bearbeitete Zeit: 27. Juni 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AWSAppFabricReadOnlyAccess

`AWSAppFabricReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf die AWS AppFabric

Verwendung dieser Richtlinie

Sie können Verbindungen `AWSAppFabricReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 19:52 UTC
- Bearbeitete Zeit: 27. Juni 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AWSAppFabricServiceRolePolicy

`AWSAppFabricServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: In Ihrem Namen AppFabric Zugriff auf AWS Ressourcen gewährt

Verwendung dieser Richtlinie

Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen auszuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstverknüpfte Rollen
- Erstellungszeit: 26. Juni 2023, 21:07 UTC
- Bearbeitete Zeit: 26. Juni 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AWSApplicationAutoscalingAppStreamFleetPolicy

`AWSApplicationAutoscalingAppStreamFleetPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen gewährt AppStream und CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die servicegebundene Rolle zugeordnet, die die servicegebundene Rolle zugeordnet, die die servicegebundene Rolle zugeordnet, die die servicegebundene Rolle Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 20. Oktober 2017, 19:04 UTC
- Bearbeitete Zeit: 20. Oktober 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Richtlinie, die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingCassandraTablePolicy

`AWSApplicationAutoscalingCassandraTablePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Cassandra gewährt und CloudWatch.

Verwenden diese Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. März 2020, 22:49 UTC
- Bearbeitete Zeit: 18. März 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingComprehendEndpointPolicy

`AWSApplicationAutoscalingComprehendEndpointPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Comprehend und gewährt CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 14. November 2019, 18:39 UTC
- Bearbeitete Zeit: 14. November 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoScalingCustomResourcePolicy

`AWSApplicationAutoScalingCustomResourcePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinien, die Application Auto Scaling Berechtigungen für den Zugriff auf ApiGateway und CloudWatch für die benutzerdefinierte Ressourcenskalierung gewähren

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 4. Juni 2018, 23:22 UTC
- Bearbeitete Zeit: 4. Juni 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSApplicationAutoscalingDynamoDBTablePolicy

`AWSApplicationAutoscalingDynamoDBTablePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf DynamoDB gewährt und CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 20. Oktober 2017 21:34 UTC
- Bearbeitete Zeit: 20. Oktober 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf EC2 Spot Fleet gewährt und CloudWatch.

Verwenden Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 25. Oktober 2017, 18:23 UTC
- Bearbeitete Zeit: 25. Oktober 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

dokument dokument dokument dokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS

AWSApplicationAutoscalingECSServicePolicy

`AWSApplicationAutoscalingECSServicePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf den EC2 Container Service gewährt und CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 25. Oktober 2017, 23:53 UTC
- Bearbeitete Zeit: 25. Oktober 2017, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtelement

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingElastiCacheRGPolicy

`AWSApplicationAutoscalingElastiCacheRGPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Amazon ElastiCache und Amazon gewährt CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 17. August 2021, 23:41 UTC
- Bearbeitete Zeit: 17. August 2021, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingEMRInstanceGroupPolicy

`AWSApplicationAutoscalingEMRInstanceGroupPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Elastic Map Reduce gewährt und CloudWatch.

Verwenden von dieser Richtlinie mit dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. Oktober 2017, 00:57 UTC
- Bearbeitete Zeit: 26. Oktober 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
```

```
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinie und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingKafkaClusterPolicy

`AWSApplicationAutoscalingKafkaClusterPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Managed Streaming for Apache Kafka gewährt und CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 24. August 2020, 18:36 UTC
- Bearbeitete Zeit: 24. August 2020, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die -Version definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richt

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingLambdaConcurrencyPolicy

`AWSApplicationAutoscalingLambdaConcurrencyPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Lambda gewährt und CloudWatch.

Verwenden mit dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. Oktober 2019, 20:04 UTC
- Bearbeitete Zeit: 21. Oktober 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die StandardVersion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinien

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

```
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen angehängt

AWSApplicationAutoscalingNeptuneClusterPolicy

`AWSApplicationAutoscalingNeptuneClusterPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Amazon Neptune und Amazon gewährt CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 2. September 2021, 21:14 UTC
- Bearbeitete Zeit: 2. September 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingRDSClusterPolicy

`AWSApplicationAutoscalingRDSClusterPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf RDS gewährt und CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. Oktober 2017, 17:46 UTC
- Bearbeitete Zeit: 7. August 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

Dokument mit -Richtlinien

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationAutoscalingSageMakerEndpointPolicy

`AWSApplicationAutoscalingSageMakerEndpointPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen gewährt SageMaker und CloudWatch.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. Februar 2018, 19:58 UTC
- Bearbeitete Zeit: 13. November 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationDiscoveryAgentAccess

`AWSApplicationDiscoveryAgentAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht dem Discovery Agent den Zugriff auf die Registrierung beimAWS Application Discovery Service.

Verwenden dieser Richtlinie

Sie können`AWSApplicationDiscoveryAgentAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Mai 2016, 21:38 UTC
- Bearbeitete Zeit: 24. Februar 2020, 22:26 UTC

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

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSApplicationDiscoveryAgentlessCollectorAccess

`AWSApplicationDiscoveryAgentlessCollectorAccess`ist eine AWSverwaltete Richtlinie, die: Application Discovery Service Agentless Collectors die auto Aktualisierung, Registrierung und Kommunikation mit Application Discovery Service ermöglicht

Verwenden dieser Richtlinie

Sie können`AWSApplicationDiscoveryAgentlessCollectorAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 16. August 2022, 21:00 UTC
- Bearbeitete Zeit: 16. August 2022, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationDiscoveryServiceFullAccess

`AWSApplicationDiscoveryServiceFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf die Anzeige und Kennzeichnung von Konfigurationselementen bietet, die vomAWS Application Discovery Service verwaltet werden

Verwenden dieser Richtlinie

Sie können`AWSApplicationDiscoveryServiceFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Mai 2016, 21:30 UTC
- Bearbeitete Zeit: 19. Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Richtlinien mit den geringsten Berechtigungen

AWSApplicationMigrationAgentInstallationPolicy

`AWSApplicationMigrationAgentInstallationPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Installation desAWS Replication Agents, der zusammen mit demAWS Application Migration Service (MGN) verwendet wird, um externe Server zu migrierenAWS. Hängen Sie diese Richtlinie an Ihre IAM-Benutzer oder -Rollen an, deren Anmeldeinformationen Sie bei der Installation desAWS Replication Agents angeben.

Verwenden dieser -Richtlinie

Sie können`AWSApplicationMigrationAgentInstallationPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Juni 2022, 07:51 UTC
- Bearbeitete Zeit: 20. September 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf verwaltete Berechtigungen

AWSApplicationMigrationAgentPolicy

`AWSApplicationMigrationAgentPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Installation und Verwendung desAWS Replication Agents, der zusammen mit demAWS Application Migration Service (MGN) für die Migration externer Server verwendet wirdAWS. Hängen Sie diese Richtlinie an Ihre IAM-Benutzer oder -Rollen an, deren Anmeldeinformationen Sie bei der Installation desAWS Replication Agents angeben.

Verwenden dieser -Richtlinie

Sie können`AWSApplicationMigrationAgentPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. April 2021, 07:00 UTC
- Bearbeitete Zeit: 20. September 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSApplicationMigrationAgentPolicy_v2

`AWSApplicationMigrationAgentPolicy_v2`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Verwendung desAWS Replication Agents, der zusammen mit demAWS Application Migration Service (MGN) verwendet wird, um externe Server zu migrierenAWS. Wir empfehlen jedoch nicht, dass Sie diese -Richtlinie Ihren IAM-Benutzern oder -Rollen hinzufügen.

Verwenden dieser -Richtlinie

Sie können`AWSApplicationMigrationAgentPolicy_v2` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Juni 2022, 14:14 UTC
- Bearbeitete Zeit: 6. Juni 2022, 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationMigrationConversionServerPolicy

`AWSApplicationMigrationConversionServerPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es dem Application Migration Service (MGN) Conversion Server, bei denen es sich um EC2-Instances handelt, die vom Application Migration Service gestartet wurden, mit dem MGN-Dienst zu kommunizieren. Eine IAM-Rolle mit dieser Richtlinie wird (als EC2-Instanzprofil) von MGN an die MGN Conversion Server angehängt, die bei Bedarf automatisch von MGN gestartet und beendet werden. Wir empfehlen jedoch nicht, dass Sie diese -Richtlinie Ihren IAM-Benutzern oder -Rollen hinzufügen. MGN Conversion Server werden vom Application Migration

Service verwendet, wenn Benutzer Test- oder Cutover-Instances über die MGN-Konsole, CLI oder API starten möchten.

Verwenden dieser -Richtlinie

Sie könnenAWSApplicationMigrationConversionServerPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 7. April 2021, 06:48 UTC
- Bearbeitete Zeit: 7. April 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf die Richtlinien und Umstellung auf Berechtigungen mit den -verwaltete Berechtigungen

AWSApplicationMigrationEC2Access

`AWSApplicationMigrationEC2Access`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie bietet Amazon EC2 EC2-Operationen, die erforderlich sind, um den Application Migration Service (MGN) zu verwenden, um die migrierten Server als EC2-Instances zu starten. Hängen Sie diese Richtlinie an Ihre IAM-Benutzer oder -Rollen an.

Verwenden dieser Richtlinien

Sie können`AWSApplicationMigrationEC2Access` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. April 2021, 07:05 UTC
- Bearbeitete Zeit: 06. Februar 2023, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationMigrationFullAccess

`AWSApplicationMigrationFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen für alle öffentlichen APIs desAWS Application Migration Service (MGN) sowie Berechtigungen zum Lesen von KMS-Schlüsselinformationen. Hängen Sie diese Richtlinie an Ihre IAM-Benutzer oder -Rollen an.

Verwenden von -Richtlinie von Richtlinie mit

Sie können`AWSApplicationMigrationFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. April 2021, 06:56 UTC
- Bearbeitete Zeit: 20. April 2023, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Richtlinie definiert die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JAM-Richtlinie Richtlinie JAM-Richtlinie

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von IAM-AM-AM-AM-AM-AM-AM-AM-AM-AM-AM-Richtlinie
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinie und Umstellung auf die geringsten Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen Berechtigungen die geringsten Berechtigungen Berechtigungen Berechtigungen Berechtigungen

AWSApplicationMigrationMGHAccess

`AWSApplicationMigrationMGHAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht esAWS Application Migration Service (MGN), Metadaten über den Fortschritt der Server, die mithilfe von MGN migriert werden, an denAWS Migration Hub (MGH) zu senden. MGN erstellt automatisch eine IAM-Rolle mit dieser angehängten Richtlinie und übernimmt diese Rolle. Wir empfehlen jedoch nicht, dass Sie diese -Richtlinie an IAM-Benutzer oder -Rollen anhängen.

Verwenden dieser Richtlinie von Verwenden dieser Richtlinie

Sie können`AWSApplicationMigrationMGHAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 7. April 2021, 07:10 UTC
- Bearbeitete Zeit: 7. April 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument.

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von IAM-Identitätsberechtigungen und -IAM-Identitätsberechtigungen hinzufügen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen von -Least-Privilege-Richtlinien.

AWSApplicationMigrationReadOnlyAccess

`AWSApplicationMigrationReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen für alle schreibgeschützten öffentlichen APIs des Application Migration Service (MGN) sowie für einige schreibgeschützte APIs andererAWS Dienste, die erforderlich sind, um die MGN-Konsole vollständig schreibgeschützt zu nutzen. Hängen Sie diese Richtlinie an Ihre IAM-Benutzer oder -Rollen an.

Verwenden dieser Richtlinie

Sie können`AWSApplicationMigrationReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. April 2021, 07:15 UTC
- Bearbeitete Zeit: 20. März 2023, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationMigrationReplicationServerPolicy

`AWSApplicationMigrationReplicationServerPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es den Application Migration Service (MGN) Replication Servern, bei denen es sich um EC2-Instances handelt, die vom Application Migration Service gestartete EC2-Instances, mit dem MGN-Service zu kommunizieren und EBS-Snapshots in Ihrem zu erstellenAWS-Konto. Eine IAM-Rolle mit dieser Richtlinie wird (als EC2-Instanzprofil) vom Application Migration Service an die MGN Replication Server angehängt, die von MGN je nach Bedarf automatisch

gestartet und beendet werden. MGN-Replikationsserver werden verwendet, um im Rahmen des mit MGN verwalteten Migrationsprozesses die Datenreplikation von Ihren externen Servern zuAWS erleichtern. Wir empfehlen jedoch nicht, dass Sie diese -Richtlinie Ihren IAM-Benutzern oder -Rollen verwenden.

Verwenden dieser Richtlinie von dieser Richtlinie von

Sie könnenAWSApplicationMigrationReplicationServerPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 7. April 2021, 07:21 UTC
- Bearbeitete Zeit: 7. April 2021, 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie definiert die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument.

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von von IAM-Identitätsberechtigungen von IAM-Identitätsberechtigungen von
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte verwalteter Richtlinien und Umstellung auf Berechtigungen mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen verwalteter Richtlinien und Umstellung auf Berechtigungen verwalteter Richtlinien

AWSApplicationMigrationServiceEc2InstancePolicy

`AWSApplicationMigrationServiceEc2InstancePolicy` ist eine von AWS verwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS Replikationsagenten, der vom AWS Application Migration Service (AWS MGN) verwendet wird, um Quellserver zu migrieren, die auf EC2 (regionsübergreifend oder AZ-übergreifend) ausgeführt werden. Eine IAM-Rolle mit dieser Richtlinie sollte (als EC2-Instance-Profil) an die EC2-Instances angehängt werden.

Verwenden dieser Richtlinie

Sie können `AWSApplicationMigrationServiceEc2InstancePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 22. August 2023, 13:19 UTC
- Bearbeitungszeit: 03. Januar 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationServiceRolePolicy

`AWSApplicationMigrationServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es dem AWS Application Migration Service ermöglicht, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

Verwendung dieser Richtlinie

Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen auszuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstverknüpfte Rollen
- Aufnahmezeit: 7. April 2021, 06:43 UTC
- Bearbeitete Zeit: 20. Juni 2023, 09:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AWSApplicationMigrationSSMAccess

`AWSApplicationMigrationSSMAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie bietet Zugriff auf Amazon SSM-Operationen, die erforderlich sind, um den Application Migration Service (MGN) zur Ausführung benutzerdefinierter SSM-Dokumente mit Befehlen nach der Migration zu verwenden. Hängen Sie diese Richtlinie an Ihre IAM-Benutzer oder -Rollen an.

Verwenden dieser -Richtlinie

Sie könnenAWSApplicationMigrationSSMAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2022, 09:29 UTC
- Bearbeitete Zeit: 20. März 2023, 10:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete Version ist die -verwaltete Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSApplicationMigrationVCenterClientPolicy

`AWSApplicationMigrationVCenterClientPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Installation und Verwendung desAWS vCenter Client, der zusammen mit demAWS Application Migration Service (MGN) verwendet wird, um externe Server zu migrierenAWS. Hängen Sie diese Richtlinie an Ihre IAM-Benutzer oder -Rollen an, deren Anmeldeinformationen Sie bei der Installation desAWS vCenter Client angeben.

Verwenden dieser -Richtlinie

Sie können`AWSApplicationMigrationVCenterClientPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 8. November 2021, 12:53 UTC
- Bearbeitete Zeit: 8. November 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppMeshEnvoyAccess

`AWSAppMeshEnvoyAccess`ist eine AWSverwaltete Richtlinie, die: App Mesh Envoy-Richtlinie für den Zugriff auf die Virtual Node-Konfiguration.

Verwenden dieser -Richtlinie

Sie können`AWSAppMeshEnvoyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Juli 2019, 21:29 UTC
- Bearbeitete Zeit: 3. Juli 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppMeshFullAccess

`AWSAppMeshFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf dieAWS App Mesh Mesh-APIs und die Management Console bietet.

Verwenden dieser -Richtlinie

Sie können`AWSAppMeshFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 16. April 2019, 17:50 UTC
- Bearbeitete Zeit: 7. Januar 2021, 19:54 UTC

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

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppMeshPreviewEnvoyAccess

`AWSAppMeshPreviewEnvoyAccess`ist eine AWSverwaltete Richtlinie, die: App Mesh Preview Envoy-Richtlinie für den Zugriff auf die Virtual Node-Konfiguration.

Verwenden dieser Richtlinien

Sie könnenAWSAppMeshPreviewEnvoyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. August 2019, 23:32 UTC
- Bearbeitete Zeit: 5. August 2019, 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen, die die Berechtigungen für die -verwaltete Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppMeshPreviewServiceRolePolicy

`AWSAppMeshPreviewServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und die vonAWS App Mesh verwendeten oder verwalteten Ressourcen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. Juni 2019, 19:07 UTC
- Bearbeitete Zeit: 21. August 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON----Richtlinie

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

```
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Berechtigungen

AWSAppMeshReadOnly

`AWSAppMeshReadOnly`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf dieAWS App Mesh Mesh-APIs und die Management Console bietet.

Verwenden dieser -Richtlinie

Sie können`AWSAppMeshReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 16. April 2019, 17:51 UTC
- Bearbeitete Zeit: 7. Januar 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppMeshServiceRolePolicy

`AWSAppMeshServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff AWS-Services auf Ressourcen ermöglicht, die von verwendet oder verwaltet werden AWS AppMesh

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Juni 2019, 18:30 Uhr UTC
- Bearbeitete Zeit: 10. Oktober 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppRunnerFullAccess

`AWSAppRunnerFullAccess`ist eine AWSverwaltete Richtlinie, die: Berechtigungen für alle App Runner-Aktionen gewährt.

Verwenden dieser Richtlinien

Sie könnenAWSAppRunnerFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Januar 2022, 04:02 UTC
- Bearbeitete Zeit: 11. Januar 2022, 04:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppRunnerReadOnlyAccess

`AWSAppRunnerReadOnlyAccess`ist eine AWS-verwaltete -Richtlinie, die: Berechtigungen zum Auflisten und Anzeigen von Details zu App-Runner-Ressourcen -Ressourcen.

Verwenden dieser Richtlinien

Sie können`AWSAppRunnerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Februar 2022, 21:24 UTC
- Bearbeitete Zeit: 24. Februar 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die Version, die die Berechtigungen für die -Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-IdentitätsBerechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit -verwaltete Richtlinien und Umstellung auf Berechtigungen mit -verwaltete Richtlinien

AWSAppRunnerServicePolicyForECRAccess

`AWSAppRunnerServicePolicyForECRAccess`ist eine AWSverwaltete Richtlinie, die:AWS App Runner-Servicerichtlinie, die Leseberechtigungen für Amazon ECR-Ressourcen im Kundenkonto

gewährt. Verwenden Sie es in einer Rolle, die an App Runner übergeben wird, wenn Sie einen App Runner-Dienst erstellen oder aktualisieren.

Verwenden dieser -Richtlinie

Sie könnenAWSAppRunnerServicePolicyForECRAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. Mai 2021, 19:17 UTC
- Bearbeitete Zeit: 14. Mai 2021, 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppSyncAdministrator

`AWSAppSyncAdministrator`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff auf den AppSync Dienst gewährt, für den Zugriff über die Konsole jedoch nicht ausreicht.

Verwenden dieser -Richtlinie

Sie können`AWSAppSyncAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. März 2018 21:20 UTC
- Bearbeitete Zeit: 4. November 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSAppSyncInvokeFullAccess

`AWSAppSyncInvokeFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Aufrufzugriff auf den AppSync Dienst bietet — sowohl über die Konsole als auch unabhängig

Verwenden dieser -Richtlinie

Sie können`AWSAppSyncInvokeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. März 2018, 21:21 UTC
- Bearbeitete Zeit: 20. März 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppSyncPushToCloudWatchLogs

`AWSAppSyncPushToCloudWatchLogs`ist eine AWSverwaltete Richtlinie, die: Ermöglicht AppSync das Senden von Protokollen an das CloudWatch Benutzerkonto.

Verwenden dieser -Richtlinie

Sie können`AWSAppSyncPushToCloudWatchLogs` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie

- Aufnahmezeit: 9. April 2018, 19:38 UTC
- Bearbeitete Zeit: 9. April 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppSyncSchemaAuthor

`AWSAppSyncSchemaAuthor`ist eine AWSverwaltete Richtlinie, die: Zugriff auf das Erstellen, Aktualisieren und Abfragen des Schemas bietet.

Verwenden dieser -Richtlinie

Sie können`AWSAppSyncSchemaAuthor` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. März 2018, 21:21 UTC
- Bearbeitete Zeit: 1. Februar 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAppSyncServiceRolePolicy

`AWSAppSyncServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS Dienste und Ressourcen ermöglicht, die verwendet oder verwaltet werden von AppSync

Verwenden dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 21. Januar 2020, 19:56 UTC
- Bearbeitete Zeit: 21. Januar 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSArtifactAccountSync

`AWSArtifactAccountSync`ist eine AWSverwaltete Richtlinie, die:AWS Artifact den schreibgeschützten Zugriff auf Operationen inAWS Organizations ermöglicht.

Verwenden dieser Richtlinie

Sie können`AWSArtifactAccountSync` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 10. April 2018, 23:04 UTC
- Bearbeitete Zeit: 10. April 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSArtifactReportsReadOnlyAccess

`AWSArtifactReportsReadOnlyAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf die AWS Artifact-Serviceberichte.

Verwenden dieser Richtlinie

Sie können `AWSArtifactReportsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 02. Januar 2024, 22:42 UTC
- Bearbeitungszeit: 02. Januar 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSArtifactServiceRolePolicy

`AWSArtifactServiceRolePolicy`ist einAWSverwaltete Richtliniedas: ErlaubtAWSArtefakt zum Sammeln von Informationen über eine Organisation überAWSService für Organisationen.

Diese Richtlinie verwenden

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für dienstbezogene Rollen
- Zeitpunkt der Erstellung: 21. August 2023, 20:27 Uhr UTC
- Bearbeitete Zeit:21. August 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
```

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSAuditManagerAdministratorAccess

`AWSAuditManagerAdministratorAccess`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff bietet, umAWS Audit Manager zu aktivieren oder zu deaktivieren, Einstellungen zu aktualisieren und Bewertungen, Kontrollen und Frameworks zu verwalten

Verwenden dieser Richtlinien

Sie können`AWSAuditManagerAdministratorAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Dezember 2020, 20:02 UTC
- Bearbeitete Zeit: 30. April 2022, 00:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSAuditManagerServiceRolePolicy

`AWSAuditManagerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf AWS-Services und die von AWS Audit Manager verwendeten oder verwalteten Ressourcen ermöglicht

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Dezember 2020, 15:12 Uhr UTC
- Bearbeitete Zeit: 6. Dezember 2023, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListModelCustomizationJobs",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
```

```
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
```

```
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "rds:DescribeCertificates",
        "rds:DescribeDbClusterEndpoints",
        "rds:DescribeDbClusterParameterGroups",
        "rds:DescribeDbClusters",
        "rds:DescribeDBInstances",
        "rds:DescribeDbSecurityGroups",
        "redshift:DescribeClusters",
        "route53:GetQueryLoggingConfig",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "securityhub:DescribeStandards",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf:ListActivatedRulesInRuleGroup"
      ],
      "Resource" : "*",
      "Sid" : "AuditManagerAPICallAccess"
    },
    {
      "Sid" : "AuditManagerS3GetBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:source" : "false"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
```

```
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAutoScalingPlansEC2AutoScalingPolicy

`AWSAutoScalingPlansEC2AutoScalingPolicy`ist eine AWSverwaltete Richtlinie, die: Eine Richtlinie, dieAWS Auto Scaling Berechtigungen gewährt, um in einem Skalierungsplan regelmäßig Kapazitätsprognosen und geplante Skalierungsaktionen für Auto Scaling-Gruppen zu generieren

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 23. August 2018, 22:46 UTC
- Bearbeitete Zeit: 23. August 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBackupAuditAccess

`AWSBackupAuditAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Benutzern die Berechtigung, Kontrollen und Frameworks zu erstellen, die ihre Erwartungen anAWS Backup-Ressourcen und -Aktivitäten definieren, undAWS Backup-Ressourcen und -Aktivitäten anhand ihrer definierten Kontrollen und Frameworks zu überprüfen. Diese Richtlinie gewährtAWS Config und ähnlichen Diensten Berechtigungen, um die Erwartungen der Benutzer zu beschreiben und die Audits durchzuführen. Diese Richtlinie gewährt auch Berechtigungen zur Übermittlung von Prüfberichten an S3 und ähnliche Dienste und ermöglicht es Benutzern, ihre Auditberichte zu finden und zu öffnen.

Verwenden dieser Richtlinie

Sie könnenAWSBackupAuditAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. August 2021, 01:02 UTC
- Bearbeitete Zeit: 10. April 2023, 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupAuditAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie definiert die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBackupDataTransferAccess

`AWSBackupDataTransferAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es demAWS Backint-Agenten, die Backup-Datenübertragung mit derAWS Backup-Speicherebene abzuschließen. Hängen Sie diese Richtlinie an Rollen an, die von EC2-Instances übernommen werden, auf denen SAP HANA mit dem Backint-Agenten ausgeführt wird.

Verwenden dieser -Richtlinie

Sie können`AWSBackupDataTransferAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 10. November 2022, 22:48 UTC
- Bearbeitete Zeit: 10. November 2022, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBackupFullAccess

`AWSBackupFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie richtet sich an Backup-Administratoren und gewährt vollen Zugriff auf AWS Backup-Operationen, einschließlich der Erstellung oder Bearbeitung von Backup-Plänen, der Zuweisung von AWS Ressourcen zu Backup-Plänen, dem Löschen von Backups und dem Wiederherstellen von Backups.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. November 2019, 22:21 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`ist eine AWSverwaltete Richtlinie, die:AWS BackupGateway Erlaubt, die Metadaten virtueller Maschinen in Ihrem Namen zu synchronisieren

Verwenden dieser -Richtlinie

Sie können`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 15. Dezember 2022, 19:43 UTC
- Bearbeitete Zeit: 15. Dezember 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die -Standardversion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSBackupOperatorAccess

`AWSBackupOperatorAccess`ist einAWSverwaltete Richtliniedas: Diese Richtlinie gewährt Benutzern ZuweisungsberechtigungenAWSRessourcen für Backup-Pläne, Erstellung von On-Demand-Backups und Wiederherstellung von Backups. Diese Richtlinie erlaubt es dem Benutzer nicht, Backup-Pläne zu erstellen oder zu bearbeiten oder geplante Backups zu löschen, nachdem sie erstellt wurden.

Verwenden Sie diese Richtlinie

Sie können anhängen`AWSBackupOperatorAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie
- Zeitpunkt der Erstellung: 18. November 2019, 22:23 Uhr UTC
- Bearbeitete Zeit:6. September 2023, 20:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Version der Richtlinie

Version der Richtlinie: v15(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSBackupOrganizationAdminAccess

`AWSBackupOrganizationAdminAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie richtet sich an Backup-Administratoren, die das kontoübergreifende Backup-Management verwenden, um Backups für das Unternehmen zu verwalten.

Verwenden dieser Richtlinien

Sie können`AWSBackupOrganizationAdminAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2020, 16:23 UTC
- Bearbeitete Zeit: 18. November 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument


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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBackupRestoreAccessForSAPHANA

`AWSBackupRestoreAccessForSAPHANA`ist eine AWSverwaltete Richtlinie, die: Erteilt dieAWS Backup-Berechtigung zur Wiederherstellung einer Sicherung von SAP HANA auf Amazon EC2

Verwenden dieser Richtlinien

Sie können`AWSBackupRestoreAccessForSAPHANA` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 10. November 2022, 22:43 UTC
- Bearbeitete Zeit: 10. November 2022, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte und Umstellung auf Berechtigungen

AWSBackupServiceLinkedRolePolicyForBackup

`AWSBackupServiceLinkedRolePolicyForBackup`ist eine AWSverwaltete Richtlinie, die: Die AWS Backup-Berechtigung zum Erstellen von Backups in Ihrem Namen für verschiedene AWS Dienste gewährt

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Juni 2020, 23:08 UTC
- Bearbeitete Zeit: 15. Dezember 2023, 22:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceLinkedRolePolicyForBackupTest

`AWSBackupServiceLinkedRolePolicyForBackupTest`ist eine AWSverwaltete Richtlinie, die:AWS Backups die Berechtigung erteilt, Backups in Ihrem NamenAWS dienstübergreifend zu erstellen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. Mai 2020, 17:37 UTC
- Bearbeitete Zeit: 12. Mai 2020, 17:37 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die die die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBackupServiceRolePolicyForBackup

`AWSBackupServiceRolePolicyForBackup`ist eine AWSverwaltete Richtlinie, die: Die AWS Backup-Berechtigung zum Erstellen von Backups in Ihrem Namen für alle AWS Dienste gewährt

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSBackupServiceRolePolicyForBackup` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. Januar 2019, 21:01 UTC
- Bearbeitete Zeit: 15. Dezember 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Version der Richtlinie

Richtlinienversion: v18 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForRestores

`AWSBackupServiceRolePolicyForRestores`ist eine AWSverwaltete Richtlinie, die: AWS Backup-Berechtigungen erteilt, um in Ihrem Namen wiederherzustellende AWS Dienste durchzuführen. Diese Richtlinie umfasst Berechtigungen zum Erstellen und Löschen von AWS Ressourcen wie EBS-Volumes, RDS-Instances und EFS-Dateisystemen, die Teil des Wiederherstellungsprozesses sind.

Verwenden dieser Richtlinie

Sie können Verbindungen `AWSBackupServiceRolePolicyForRestores` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. Januar 2019, 00:23 UTC
- Bearbeitete Zeit: 15. Dezember 2023, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Version der Richtlinie

Richtlinienversion: v20 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForS3Backup

`AWSBackupServiceRolePolicyForS3Backup`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die Berechtigungen enthält, die fürAWS Backup erforderlich sind, um Daten in einem beliebigen S3-Bucket zu sichern. Dies beinhaltet den Lesezugriff auf alle S3-Objekte und den Entschlüsselungszugriff für alle KMS-Schlüssel.

Verwenden dieser -Richtlinie

Sie können`AWSBackupServiceRolePolicyForS3Backup` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Februar 2022, 17:40 UTC

- Bearbeitete Zeit: 1. September 2022, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBackupServiceRolePolicyForS3Restore

`AWSBackupServiceRolePolicyForS3Restore`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie enthält die Berechtigungen, dieAWS Backup benötigt, um ein S3-Backup in einem Bucket wiederherzustellen. Dazu gehören Lese-/Schreibberechtigungen für alle S3-Buckets sowie Berechtigungen DescribeKey für GenerateDataKey und für alle KMS-Schlüssel.

Verwenden dieser Richtlinie

Sie können`AWSBackupServiceRolePolicyForS3Restore` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Februar 2022, 17:39 UTC
- Bearbeitete Zeit: 7. Februar 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBatchFullAccess

`AWSBatchFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Batch-Ressourcen bietet.

Verwenden dieser -Richtlinie

Sie können`AWSBatchFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 6. Dezember 2016, 19:35 UTC
- Bearbeitete Zeit: 24. Oktober 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBatchServiceEventTargetRole

`AWSBatchServiceEventTargetRole`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung von CloudWatch Event Target für dieAWS Batch-Auftragsübermittlung

Verwenden dieser -Richtlinie

Sie können`AWSBatchServiceEventTargetRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 28. Februar 2018, 22:31 UTC
- Bearbeitete Zeit: 28. Februar 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Richtlinien. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und auf auf mit den geringsten Berechtigungen

AWSBatchServiceRole

`AWSBatchServiceRole`ist eine AWSverwaltete Richtlinie, die: Richtlinie für die AWS Batch-Servicerolle, die den Zugriff auf verwandte Dienste wie EC2, Autoscaling, EC2 Container Service und Cloudwatch Logs ermöglicht.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBatchServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Dezember 2016, 19:36 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBillingConductorFullAccess

`AWSBillingConductorFullAccess`ist eine AWSverwaltete Richtlinie, die: Verwenden Sie die AWSBillingConductorFullAccess verwaltete Richtlinie, um den vollständigen Zugriff auf dieAWS Billing Conductor (ABC-) Konsole und APIs zu ermöglichen. Diese Richtlinie ermöglicht es Benutzern, ABC-Ressourcen aufzulisten, zu erstellen und zu löschen.

Verwenden dieser -Richtlinie

Sie können`AWSBillingConductorFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. April 2022, 18:02 UTC
- Bearbeitete Zeit: 13. April 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die Version, die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf die geringsten ste ste ste ste ste ste ste Berechtigungen

AWSBillingConductorReadOnlyAccess

`AWSBillingConductorReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Verwenden Sie die AWSBillingConductorReadOnlyAccess verwaltete Richtlinie, um nur Lesezugriff auf dieAWS Billing Conductor (ABC-) Konsole und APIs zu gewähren. Diese Richtlinie gewährt die Berechtigung zum Abrufen und Auflisten aller ABC-Ressourcen. Sie umfasst nicht die Möglichkeit, Ressourcen zu erstellen oder auf Ressourcen zuzugreifen.

Verwenden dieser Richtlinie

Sie können`AWSBillingConductorReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. April 2022, 18:02 UTC
- Bearbeitete Zeit: 13. April 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBillingReadOnlyAccess

`AWSBillingReadOnlyAccess` ist eine -AWSverwaltete Richtlinie, die Benutzern das Anzeigen von Rechnungen in der -Fakturierungskonsole ermöglicht.

Verwenden dieser Richtlinie

Sie können `AWSBillingReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 27. August 2020, 20:08 UTC
- Bearbeitungszeit: 17. Januar 2024, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen zur Steuerung vonAWS Ressourcen. Sie können beispielsweiseAWS Systems Manager (SSM) -Skripte ausführen und stoppen.

Verwenden dieser -Richtlinie

Sie können`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. Mai 2022, 19:03 UTC
- Bearbeitete Zeit: 25. Mai 2022, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -verwaltete -verwaltete Version für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBudgetsActionsWithAWSResourceControlAccess

`AWSBudgetsActionsWithAWSResourceControlAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS Budgets Actions gewährt, einschließlich der Verwendung von Budgets Actions zur Kontrolle des Zustands laufenderAWS Ressourcen überAWS Management Console

Verwenden dieser -Richtlinie

Sie können`AWSBudgetsActionsWithAWSResourceControlAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Oktober 2020, 17:19 UTC
- Bearbeitete Zeit: 15. Oktober 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Standardversion ist die -verwaltete Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS

Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AWSBudgetsReadOnlyAccess

`AWSBudgetsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Über den nur Lesezugriff auf dieAWS Budgets Console gewährtAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AWSBudgetsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Oktober 2020, 17:18 UTC
- Bearbeitete Zeit: 15. Oktober 2020, 17:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AWSBugBustFullAccess

`AWSBugBustFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese IAM-Richtlinie gewährt Benutzern vollen Zugriff auf dieAWS BugBust Konsole

Verwenden dieser -Richtlinie

Sie könnenAWSBugBustFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2021, 07:03 UTC
- Bearbeitete Zeit: 22. Juli 2021, 20:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSBugBustPlayerAccess

`AWSBugBustPlayerAccess`ist eine AWSverwaltete Richtlinie, die: Diese IAM-Richtlinie gewährt Benutzern Zugriff auf die Teilnahme anAWS BugBust Veranstaltungen

Verwenden von dieser Richtlinie

Sie könnenAWSBugBustPlayerAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2021, 07:15 UTC
- Bearbeitete Zeit: 24. Juni 2021, 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Version definiert die Berechtigungen für die -verwaltete Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSBugBustServiceRolePolicy

`AWSBugBustServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen für denAWS BugBust Zugriff auf Ressourcen in Ihrem Namen gewährt

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 24. Juni 2021, 06:59 UTC
- Bearbeitete Zeit: 24. Juni 2021, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf denAWS Certificate Manager (ACM) bietet

Verwenden dieser -Richtlinie

Sie können`AWSCertificateManagerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. Januar 2016, 17:02 UTC
- Bearbeitete Zeit: 17. August 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCertificateManagerPrivateCAAuditor

`AWSCertificateManagerPrivateCAAuditor`ist eine AWSverwaltete Richtlinie, die: Auditoren Zugriff auf dieAWS Certificate Manager Private Certificate Authority gewährt

Verwenden dieser Richtlinien

Sie können`AWSCertificateManagerPrivateCAAuditor` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. Oktober 2018, 16:51 UTC
- Bearbeitete Zeit: 17. August 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -verwaltete Version ist die -verwaltete Version, die die Berechtigungen für die -verwaltete Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCertificateManagerPrivateCAFullAccess

`AWSCertificateManagerPrivateCAFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Certificate Manager Private Certificate Authority bietet

Verwenden dieser Richtlinien

Sie können`AWSCertificateManagerPrivateCAFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 23. Oktober 2018, 16:54 UTC
- Bearbeitete Zeit: 23. Oktober 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinien definiert die Berechtigungen für die -Richtlinie, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit denAWS geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AWSCertificateManagerPrivateCAPrivilegedUser

`AWSCertificateManagerPrivateCAPrivilegedUser`ist eine AWSverwaltete Richtlinie, die: Privilegierten Zertifikatsbenutzern Zugriff aufAWS Certificate Manager Private Certificate Authority gewährt

Verwenden dieser -Richtlinie

Sie können`AWSCertificateManagerPrivateCAPrivilegedUser` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. Juni 2019, 17:43 UTC
- Bearbeitete Zeit: 20. Juni 2019, 17:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCertificateManagerPrivateCAReadOnly

`AWSCertificateManagerPrivateCAReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS Certificate Manager Private Certificate Authority gewährt

Verwenden dieser -Richtlinie

Sie können`AWSCertificateManagerPrivateCAReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. Oktober 2018, 16:57 UTC
- Bearbeitete Zeit: 17. August 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion definiert die Berechtigungen für die -verwaltete -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCertificateManagerPrivateCAUser

`AWSCertificateManagerPrivateCAUser`ist eine AWSverwaltete Richtlinie, die: Zertifikatsbenutzern Zugriff aufAWS Certificate Manager Private Certificate Authority gewährt

Verwenden dieser -Richtlinie

Sie können`AWSCertificateManagerPrivateCAUser` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 23. Oktober 2018, 16:53 UTC
- Bearbeitete Zeit: 20. Juni 2019, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCertificateManagerReadOnly

`AWSCertificateManagerReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf denAWS Certificate Manager (ACM) gewährt.

Verwenden dieser Richtlinie

Sie können`AWSCertificateManagerReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. Januar 2016, 17:07 UTC
- Bearbeitete Zeit: 15. März 2021, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSChatbotServiceLinkedRolePolicy

`AWSChatbotServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Die vomAWS Chatbot verwendete Service Linked Role.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen angehängt.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. November 2019, 16:39 UTC
- Bearbeitete Zeit: 18. November 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCleanRoomsFullAccess

`AWSCleanRoomsFullAccess` ist eine von AWS verwaltete Richtlinie, die: Vollzugriff auf AWS Clean Rooms-Ressourcen und Zugriff auf zugehörige gewährt AWS-Services.

Verwenden dieser Richtlinie

Sie können `AWSCleanRoomsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie

- Erstellungszeit: 12. Januar 2023, 16:10 UTC
- Bearbeitungszeit: 21. März 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSCleanRoomsFullAccessNoQuerying

`AWSCleanRoomsFullAccessNoQuerying`ist einAWSverwaltete Richtliniedas: Ermöglicht vollen Zugriff aufAWSRessourcen für Clean Rooms außer für Abfragen in einer Kollaboration und Zugriff auf verwandte RessourcenAWS-Services.

Verwendung dieser Richtlinie

Sie können anhängen`AWSCleanRoomsFullAccessNoQuerying`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 12. Januar 2023, 16:12 Uhr UTC
- Uhrzeit der Bearbeitung:31. Juli 2023, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Version der Richtlinie

Version der Richtlinie: v3(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:CreateAnalysisTemplate",
```

```
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSCleanRoomsMLFullAccess

`AWSCleanRoomsMLFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf AWS Clean Rooms ML-Ressourcen und Zugriff auf verwandte RessourcenAWS-Services ermöglicht.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCleanRoomsMLFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 21:02 UTC
- Bearbeitete Zeit: 29. November 2023, 21:02 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsMLReadOnlyAccess

`AWSCleanRoomsMLReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf AWS Clean Rooms-ML-Ressourcen und schreibgeschützten Zugriff auf zugehörige Clean Rooms-Ressourcen ermöglicht AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCleanRoomsMLReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 20:55 UTC
- Bearbeitete Zeit: 29. November 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsReadOnlyAccess

`AWSCleanRoomsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Den schreibgeschützten Zugriff aufAWS Clean Rooms-Ressourcen und den schreibgeschützten Zugriff auf zugehörigeAWS Glue- und Amazon CloudWatch Logs-Ressourcen ermöglicht.

Verwenden dieser -Richtlinie

Sie können`AWSCleanRoomsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 12. Januar 2023, 16:10 UTC
- Bearbeitete Zeit: 12. Januar 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Version ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloud9Administrator

`AWSCloud9Administrator`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff auf AWS Cloud9 bietet.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloud9Administrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:17 UTC
- Bearbeitete Zeit: 11. Oktober 2023, 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9EnvironmentMember

`AWSCloud9EnvironmentMember`ist eine AWSverwaltete Richtlinie, die: die Möglichkeit bietet, in gemeinsam genutzte AWS Cloud9-Entwicklungsumgebungen eingeladen zu werden.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloud9EnvironmentMember` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:18 Uhr UTC
- Bearbeitete Zeit: 11. Oktober 2023, 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9ServiceRolePolicy

`AWSCloud9ServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Service Linked Role Policy forAWS Cloud9

Verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 30. November 2017, 13:44 UTC
- Bearbeitete Zeit: 17. Januar 2022, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die Standardlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinie
Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONSONSONSONSONSON

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit mit den geringsten

AWSCloud9SSMInstanceProfile

`AWSCloud9SSMInstanceProfile`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie wird verwendet, um einer Rolle zuzuweisen InstanceProfile , sodass Cloud9 den SSM Session Manager verwenden kann, um eine Verbindung mit der Instanz herzustellen

Verwenden dieser -Richtlinie

Sie können`AWSCloud9SSMInstanceProfile` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Mai 2020, 11:40 UTC
- Bearbeitete Zeit: 14. Mai 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloud9User

`AWSCloud9User`ist eine AWSverwaltete Richtlinie, die: Erteilt die Erlaubnis, AWS Cloud9-Entwicklungsumgebungen zu erstellen und eigene Umgebungen zu verwalten.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloud9User` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:16 UTC
- Bearbeitete Zeit: 11. Oktober 2023, 13:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudFormationFullAccess

`AWSCloudFormationFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf bietetAWS CloudFormation.

Verwenden dieser -Richtlinie

Sie können`AWSCloudFormationFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. Juli 2019, 21:50 UTC
- Bearbeitete Zeit: 26. Juli 2019, 21:50 UTC

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

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudFormationReadOnlyAccess

`AWSCloudFormationReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht den Zugriff aufAWS CloudFormation überAWS Management Console.

Verwenden dieser -Richtlinie

Sie könnenAWSCloudFormationReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 13. November 2019, 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudFrontLogger

`AWSCloudFrontLogger`ist eine AWSverwaltete Richtlinie, die: CloudFront Logger Schreibrechte für CloudWatch Logs gewährt.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. Juni 2018, 20:15 UTC
- Bearbeitete Zeit: 22. November 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie definiert die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudHSMFullAccess

`AWSCloudHSMFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alle CloudHSM-Ressourcen bietet.

Verwenden dieser Richtlinie

Sie können`AWSCloudHSMFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudHSMReadOnlyAccess

`AWSCloudHSMReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf alle CloudHSM-Ressourcen bietet.

Verwenden dieser -Richtlinie

Sie können`AWSCloudHSMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudHSMRole

`AWSCloudHSMRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für dieAWS CloudHSM-Servicerolle.

Verwenden dieser -Richtlinie

Sie können`AWSCloudHSMRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudMapDiscoverInstanceAccess

`AWSCloudMapDiscoverInstanceAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die AWS Cloud Map Discovery API ermöglicht.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudMapDiscoverInstanceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 00:02 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapFullAccess

`AWSCloudMapFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alleAWS Cloud Map-Aktionen bietet.

Verwenden dieser Richtlinie

Sie könnenAWSCloudMapFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. November 2018, 23:57 UTC
- Bearbeitete Zeit: 29. Juli 2020, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapFullAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudMapReadOnlyAccess

`AWSCloudMapReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf alle AWS Cloud Map-Aktionen gewährt.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudMapReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 23:45 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapRegisterInstanceAccess

`AWSCloudMapRegisterInstanceAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Registrantenebene auf Map-Aktionen AWS Cloud gewährt.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudMapRegisterInstanceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 00:04 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudShellFullAccess

`AWSCloudShellFullAccess`ist eine AWSverwaltete Richtlinie, die: Die NutzungAWS CloudShell mit allen Funktionen gewährt

Verwenden dieser -Richtlinie

Sie können`AWSCloudShellFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Dezember 2020, 18:07 UTC
- Bearbeitete Zeit: 15. Dezember 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudTrail_FullAccess

`AWSCloudTrail_FullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf bietetAWS CloudTrail.

Verwenden dieser Richtlinien

Sie könnenAWSCloudTrail_FullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Oktober 2020, 23:41 UTC
- Bearbeitete Zeit: 22. Februar 2021, 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCloudTrail_ReadOnlyAccess

`AWSCloudTrail_ReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf gewährtAWS CloudTrail.

Verwenden dieser -Richtlinie dieser -Richtlinie

Sie können`AWSCloudTrail_ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Juni 2022, 17:19 UTC
- Bearbeitete Zeit: 14. Juni 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument mit

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien mit -verwaltete Richtlinien mit den geringsten Berechtigungen

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie wird von der dienstgebundenen Rolle namens verwendet AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents. CloudWatch verwendet diese dienstverknüpfte Rolle, umAWS System Manager Incident Manager-Aktionen auszuführen, wenn ein CloudWatch Alarm in den Zustand ALARM wechselt. Diese Richtlinie gewährt die Erlaubnis, Aktionen in Ihrem Namen durchzuführen.

Verwenden dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie

- Aufnahmezeit: 27. April 2021, 13:30 UTC
- Bearbeitete Zeit: 27. April 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienelement

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen und Berechtigungen mit den geringsten Berechtigungen

AWSCodeArtifactAdminAccess

`AWSCodeArtifactAdminAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS CodeArtifact über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie könnenAWSCodeArtifactAdminAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 16. Juni 2020, 23:53 UTC
- Bearbeitete Zeit: 16. Juni 2020, 23:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -Richtlinie definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeArtifactReadOnlyAccess

`AWSCodeArtifactReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS CodeArtifact über die gewährtAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AWSCodeArtifactReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. Juni 2020, 21:23 UTC
- Bearbeitete Zeit: 25. Juni 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für

den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeBuildAdminAccess

`AWSCodeBuildAdminAccess`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff aufAWS CodeBuilddüber dieAWS Management Console. Hängen Sie auch AmazonS3 anReadOnlyAccessum Zugriff auf das Herunterladen von Build-Artefakten und das Anhängen von IAM zu gewährenFullAccessum die Servicerolle für zu erstellen und zu verwaltenCodeBuild.

Verwendung dieser Richtlinie

Sie können anhängen`AWSCodeBuildAdminAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 01. Dezember 2016, 19:04 Uhr UTC
- Uhrzeit der Bearbeitung:31. Juli 2023, 23:06 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Version der Richtlinie

Version der Richtlinie: v13(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
```

```
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
```

```
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSCodeBuildDeveloperAccess

`AWSCodeBuildDeveloperAccess`ist einAWSverwaltete Richtliniedas: Bietet Zugriff aufAWS CodeBuildüber dieAWS Management Console, erlaubt aber nichtCodeBuildProjektverwaltung. Hängen Sie auch AmazonS3 anReadOnlyAccessum Zugriff auf Build-Artefakte zum Herunterladen zu gewähren.

Verwendung dieser Richtlinie

Sie können anhängen`AWSCodeBuildDeveloperAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Entstehungszeit: 01. Dezember 2016, 19:02 Uhr UTC
- Uhrzeit der Bearbeitung:31. Juli 2023, 23:06 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Version der Richtlinie

Version der Richtlinie: v14(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eineAWSressource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSCodeBuildReadOnlyAccess

`AWSCodeBuildReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS CodeBuild über die gewährtAWS Management Console. Hängen Sie auch AmazonS3 anReadOnlyAccess , um den Zugriff auf Download-Build-Artefakte zu ermöglichen.

Verwenden dieser -Richtlinie

Sie können`AWSCodeBuildReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2016, 19:03 UTC
- Bearbeitete Zeit: 14. September 2020, 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v11 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeCommitFullAccess

`AWSCodeCommitFullAccess`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff aufAWS CodeCommitüber dieAWS Management Console.

Verwendung dieser Richtlinie

Sie können anhängen`AWSCodeCommitFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 09. Juli 2015, 17:02 Uhr UTC
- Uhrzeit der Bearbeitung:17. Juli 2023, 21:50 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Version der Richtlinie

Version der Richtlinie: v10(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSCodeCommitPowerUser

`AWSCodeCommitPowerUser`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff aufAWS CodeCommitRepositorys, erlaubt aber kein Löschen des Repositorys.

Verwendung dieser Richtlinie

Sie können anhängen`AWSCodeCommitPowerUser`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 09. Juli 2015, 17:06 Uhr UTC
- Uhrzeit der Bearbeitung:17. Juli 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Version der Richtlinie

Version der Richtlinie: v15(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf

eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSCodeCommitReadOnly

`AWSCodeCommitReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS CodeCommit über die gewährtAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AWSCodeCommitReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Juli 2015, 17:05 UTC
- Bearbeitete Zeit: 18. August 2021, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Version der Richtlinie

Version der Richtlinie:v11 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeDeployDeployerAccess

`AWSCodeDeployDeployerAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Registrierung und Bereitstellung einer Revision bietet.

Verwenden dieser Richtlinie

Sie können`AWSCodeDeployDeployerAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Mai 2015, 18:18 UTC
- Bearbeitete Zeit: 2. April 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS

Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeDeployFullAccess

`AWSCodeDeployFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf CodeDeploy Ressourcen bietet.

Verwenden dieser Richtlinien

Sie können`AWSCodeDeployFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Mai 2015, 18:13 UTC
- Bearbeitete Zeit: 2. April 2020, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeDeployReadOnlyAccess

`AWSCodeDeployReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf CodeDeploy Ressourcen gewährt.

Verwenden dieser -Richtlinie

Sie können`AWSCodeDeployReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Mai 2015, 18:21 UTC
- Bearbeitete Zeit: 2. April 2020, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeDeployRole

`AWSCodeDeployRole`ist einAWSverwaltete Richtliniedas: Bietet CodeDeploy Servicezugriff, um Tags zu erweitern und in Ihrem Namen mit Auto Scaling zu interagieren.

Verwenden Sie diese Richtlinie

Sie können anhängen`AWSCodeDeployRole`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Zeit der Erstellung: 4. Mai 2015, 18:05 Uhr UTC
- Bearbeitete Zeit:16. August 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Version der Richtlinie

Version der Richtlinie: v11(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Zugriffsanfrage stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForCloudFormation

`AWSCodeDeployRoleForCloudFormation`ist eine AWSverwaltete Richtlinie, die: CodeDeploy Dienstzugriff ermöglicht, um die Lambda-Funktion in Ihrem Namen aufzurufen, um die blaue/grüne Bereitstellung durchzuführen CloudFormation.

Verwenden dieser -Richtlinie

Sie können`AWSCodeDeployRoleForCloudFormation` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 19. Mai 2020, 17:12 UTC
- Bearbeitete Zeit: 19. Mai 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeDeployRoleForECS

`AWSCodeDeployRoleForECS`ist eine AWSverwaltete Richtlinie, die: CodeDeploy Serviceweiten Zugriff bietet, um in Ihrem Namen eine blaue/grüne ECS-Bereitstellung durchzuführen. Gewährt vollen Zugriff auf Support-Services, z. B. vollen Zugriff zum Lesen aller S3-Objekte, zum Aufrufen aller Lambda-Funktionen, zum Veröffentlichen in allen SNS-Themen innerhalb des Kontos und zum Aktualisieren aller ECS-Dienste.

Verwenden dieser -Richtlinie

Sie können`AWSCodeDeployRoleForECS` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2018, 20:40 UTC
- Bearbeitete Zeit: 23. September 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS mit Berechtigungen und Umstellung auf Berechtigungen mit Berechtigungen

AWSCodeDeployRoleForECSLimited

`AWSCodeDeployRoleForECSLimited`dist eine AWSverwaltete Richtlinie, die: CodeDeploy Dienstbeschränkten Zugriff bietet, um in Ihrem Namen eine blaue/grüne ECS-Bereitstellung durchzuführen.

Verwenden dieser -Richtlinie

Sie können`AWSCodeDeployRoleForECSLimited` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2018, 20:42 UTC
- Bearbeitete Zeit: 23. September 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeDeployRoleForLambda

`AWSCodeDeployRoleForLambda`ist eine AWSverwaltete Richtlinie, die: CodeDeploy Dienstzugriff ermöglicht, um in Ihrem Namen eine Lambda-Bereitstellung durchzuführen.

Verwenden dieser -Richtlinie

Sie können`AWSCodeDeployRoleForLambda` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 28. November 2017, 14:05 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeDeployRoleForLambdaLimited

`AWSCodeDeployRoleForLambdaLimited`dist eine AWSverwaltete Richtlinie, die: CodeDeploy Dienstbeschränkten Zugriff bietet, um in Ihrem Namen eine Lambda-Bereitstellung durchzuführen.

Verwenden dieser -Richtlinie

Sie können`AWSCodeDeployRoleForLambdaLimited` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 17. August 2020, 17:14 UTC
- Bearbeitete Zeit: 17. August 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodePipeline_FullAccess

`AWSCodePipeline_FullAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf AWS CodePipeline über die AWS Management Console.

Verwenden dieser Richtlinie

Sie können `AWSCodePipeline_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 03. August 2020, 22:38 UTC
- Bearbeitungszeit: 14. März 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSCodePipeline_ReadOnlyAccess

`AWSCodePipeline_ReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS CodePipeline über die gewährtAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AWSCodePipeline_ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. August 2020, 22:25 UTC

- Bearbeitete Zeit: 3. August 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodePipelineApproverAccess

`AWSCodePipelineApproverAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Anzeige und Genehmigung manueller Änderungen für alle Pipelines bietet

Verwenden dieser -Richtlinie

Sie können`AWSCodePipelineApproverAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 28. Juli 2016, 18:59 UTC
- Bearbeitete Zeit: 2. August 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung Berechtigungen mit den geringsten Berechtigungen

AWSCodePipelineCustomActionAccess

`AWSCodePipelineCustomActionAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf benutzerdefinierte Aktionen bietet, um Jobdetails (einschließlich temporärer Anmeldeinformationen) abzufragen und Statusaktualisierungen zu meldenAWS CodePipeline.

Verwenden dieser -Richtlinie

Sie können`AWSCodePipelineCustomActionAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Juli 2015, 17:02 UTC
- Bearbeitete Zeit: 9. Juli 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit denAWS geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeStarFullAccess

`AWSCodeStarFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS CodeStar über die bietetAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AWSCodeStarFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. April 2017, 16:23 UTC
- Bearbeitete Zeit: 28. März 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die Berechtigungen definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeStarNotificationsServiceRolePolicy

`AWSCodeStarNotificationsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS CodeStar Benachrichtigungen den Zugriff auf Amazon CloudWatch Events in Ihrem Namen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 5. November 2019, 16:10 UTC
- Bearbeitete Zeit: 19. März 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der Richtlinie ist die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCodeStarServiceRole

`AWSCodeStarServiceRole`ist eine AWSverwaltete Richtlinie, die: NICHT VERWENDEN —AWS CodeStar Service Role Policy, die Administratorrechte gewährt, CodeStar um IAM und andere Serviceressourcen im Namen des Kunden zu verwalten.

Verwenden dieser -Richtlinie

Sie können`AWSCodeStarServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 19. April 2017, 15:20 UTC
- Bearbeitete Zeit: 20. September 2021, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Version der Richtlinie

Version der Richtlinie:v11 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCompromisedKeyQuarantine

`AWSCompromisedKeyQuarantine`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf bestimmte Aktionen verweigert, die vomAWS Team angewendet werden, falls die Anmeldeinformationen eines IAM-Benutzers kompromittiert oder öffentlich zugänglich gemacht wurden. Entfernen Sie diese Richtlinie NICHT. Bitte folgen Sie stattdessen den Anweisungen in der E-Mail, die Sie zu dieser Veranstaltung erhalten haben.

Verwenden dieser -Richtlinie

Sie könnenAWSCompromisedKeyQuarantine an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. August 2020, 18:04 UTC
- Bearbeitete Zeit: 11. August 2020, 18:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSCompromisedKeyQuarantineV2

`AWSCompromisedKeyQuarantineV2`ist eine AWSverwaltete Richtlinie, die: Verweigert den Zugriff auf bestimmte Aktionen, die vomAWS Team angewendet werden, falls die Anmeldeinformationen eines IAM-Benutzers kompromittiert oder öffentlich zugänglich gemacht wurden. Entfernen Sie diese Richtlinie NICHT. Bitte folgen Sie stattdessen den Anweisungen, die in der für Sie erstellten Support-Anfrage zu diesem Ereignis angegeben sind.

Verwenden dieser -Richtlinie

Sie könnenAWSCompromisedKeyQuarantineV2 an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. April 2021, 22:30 UTC
- Bearbeitete Zeit: 16. März 2023, 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Berechtigungen für die Richtlinien definiert, die Berechtigungen für die Richtlinien definiert, die Berechtigungen für die Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSConfigMultiAccountSetupPolicy

`AWSConfigMultiAccountSetupPolicy`ist eine AWSverwaltete Richtlinie, die: Es Config ermöglicht,AWS Dienste aufzurufen und Konfigurationsressourcen unternehmensweit bereitzustellen

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 17. Juni 2019, 18:03
- Bearbeitete Zeit: 24. Februar 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die Standardversion der Richtlinie ist die Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinien

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

```
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSConfigRemediationServiceRolePolicy

`AWSConfigRemediationServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS Config ermöglicht, nicht konforme Ressourcen in Ihrem Namen zu korrigieren.

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 18. Juni 2019, 21:21 UTC
- Bearbeitete Zeit: 18. Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONSONSONRichtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit Richtlinien und Umstellung auf Berechtigungen

AWSConfigRoleForOrganizations

`AWSConfigRoleForOrganizations`ist eine AWSverwaltete Richtlinie, die: EsAWS Config ermöglicht, schreibgeschützteAWS Organisations-APIs aufzurufen

Verwenden dieser -Richtlinie

Sie können`AWSConfigRoleForOrganizations` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 19. März 2018, 22:53 UTC
- Bearbeitete Zeit: 24. November 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete -verwaltete -verwaltete -verwaltete Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSConfigRulesExecutionRole

`AWSConfigRulesExecutionRole`ist eine AWSverwaltete Richtlinie, die: Es einerAWS Lambda-Funktion ermöglicht, auf dieAWS Config-API und die Konfigurations-Snapshots zuzugreifen, dieAWS Config regelmäßig an Amazon S3 übermittelt. Dieser Zugriff ist für Funktionen erforderlich, die Konfigurationsänderungen für benutzerdefinierte Konfigurationsregeln auswerten.

Verwenden dieser -Richtlinie

Sie können`AWSConfigRulesExecutionRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 25. März 2016, 17:59 UTC
- Bearbeitete Zeit: 13. Mai 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie ist die die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSConfigServiceRolePolicy

`AWSConfigServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Ermöglicht Config, -AWS Services aufzurufen und Ressourcenkonfigurationen in Ihrem Namen zu erfassen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 30. Mai 2018, 23:31 UTC
- Bearbeitungszeit: 22. Februar 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v50 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen

- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSConfigUserAccess

`AWSConfigUserAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Verwendung vonAWS Config bietet, einschließlich der Suche nach Tags in Ressourcen und des Lesens aller Tags. Dies berechtigt nicht zur Konfiguration vonAWS Config, für die Administratorrechte erforderlich sind.

Verwenden dieser Richtlinie

Sie können`AWSConfigUserAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Februar 2015, 19:38 UTC
- Bearbeitete Zeit: 18. März 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSConnector

`AWSConnector` ist eine -AWS verwaltete Richtlinie, die: Ermöglicht einen breiten Lese-/Schreibzugriff auf ALLE EC2-Objekte, Lese-/Schreibzugriff auf S3-Buckets, die mit „import-to-ec2-“ beginnen, und die Möglichkeit, alle S3-Buckets aufzulisten, damit der AWS Konnektor VMs in Ihrem Namen importieren kann.

Verwenden dieser Richtlinie

Sie können `AWSConnector` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 11. Februar 2015, 17:14 UTC

- Bearbeitungszeit: 28. September 2015, 19:50 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSControlTowerAccountServiceRolePolicy

`AWSControlTowerAccountServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es dem AWS Control Tower ermöglicht, AWS Dienste anzurufen, die eine automatische Kontokonfiguration und zentrale Verwaltung in Ihrem Namen bereitstellen.

Verwenden -Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstverknüpfte Rollen
- Aufnahmezeit: 5. Juni 2023, 22:04 UTC
- Bearbeitete Zeit: 05. Juni 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion ist die Berechtigungen für die -Richtlinie, die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Verwenden -Richtlinien und Umstellung auf Berechtigungen mit AWS den geringsten Berechtigungen

AWSControlTowerServiceRolePolicy

`AWSControlTowerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff aufAWS Ressourcen gewährt, die vomAWS Control Tower verwaltet oder genutzt werden

Verwenden dieser Richtlinien

Sie können`AWSControlTowerServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 3. Mai 2019, 18:19 UTC
- Bearbeitete Zeit: 12. April 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v10 (Standard)

Die -verwaltete Richtlinien definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSCostAndUsageReportAutomationPolicy

`AWSCostAndUsageReportAutomationPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen gewährt, um die Organisation des Kontos zu beschreiben, S3-Buckets für das MAP-Programm zu erstellen und ihm Tags zuzuweisen, einen Kosten- und Nutzungsbericht zu erstellen und die Definitionen von Kosten- und Nutzungsberichten zu beschreiben.

Verwenden dieser -Richtlinie

Sie können`AWSCostAndUsageReportAutomationPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 1. November 2021, 21:27 UTC
- Bearbeitete Zeit: 1. November 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataExchangeFullAccess

`AWSDataExchangeFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Data Exchange undAWS Marketplace Aktionen mit demAWS Management Console und SDK gewährt. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, umAWS Data Exchange in vollem Umfang nutzen zu können.

Verwenden dieser -Richtlinie

Sie können`AWSDataExchangeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 2. Dezember 2021, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataExchangeProviderFullAccess

`AWSDataExchangeProviderFullAccess`ist eine AWSverwaltete Richtlinie, die: Datenanbietern Zugriff aufAWS Data Exchange undAWS Marketplace Aktionen mit demAWS Management Console und SDK gewährt. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, umAWS Data Exchange in vollem Umfang nutzen zu können.

Verwenden dieser -Richtlinie

Sie können`AWSDataExchangeProviderFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 15. März 2022, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Version der Richtlinie

Version der Richtlinie:v11 (Standard)

Die -Richtlinie definiert Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataExchangeReadOnly

`AWSDataExchangeReadOnly`ist eine AWSverwaltete Richtlinie, die: Lesezugriff aufAWS Data Exchange undAWS Marketplace Aktionen mit demAWS Management Console und SDK gewährt.

Verwenden dieser Richtlinien

Sie könnenAWSDataExchangeReadOnly an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 10. Mai 2021, 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeReadOnly

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete Version ist die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataExchangeSubscriberFullAccess

`AWSDataExchangeSubscriberFullAccess`ist eine AWSverwaltete Richtlinie, die: Datenabonnenten Zugriff aufAWS Data Exchange undAWS Marketplace Aktionen mit demAWS Management Console und SDK gewährt. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, umAWS Data Exchange in vollem Umfang nutzen zu können.

Verwenden dieser -Richtlinie

Sie können`AWSDataExchangeSubscriberFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 29. November 2021, 23:00 UTC

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

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion der -Standardrichtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataLifecycleManagerServiceRole

`AWSDataLifecycleManagerServiceRole`ist eine AWSverwaltete Richtlinie, die:AWS Data Lifecycle Manager die entsprechenden Berechtigungen gewährt, um Maßnahmen fürAWS Ressourcen zu ergreifen

Verwenden dieser Richtlinien

Sie können`AWSDataLifecycleManagerServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Juli 2018, 19:34 UTC
- Bearbeitete Zeit: 19. September 2022, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataLifecycleManagerServiceRoleForAMIManagement

`AWSDataLifecycleManagerServiceRoleForAMIManagement`ist eine AWSverwaltete Richtlinie, die:AWS Data Lifecycle Manager die entsprechenden Berechtigungen gewährt, um Aktionen anAWS Ressourcen für das AMI-Management zu ergreifen

Verwenden dieser Richtlinie

Sie können`AWSDataLifecycleManagerServiceRoleForAMIManagement` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 21. Oktober 2020, 19:39 UTC
- Bearbeitete Zeit: 19. August 2021, 17:03 UTC

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

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AWSDataLifecycleManagerSSMFullAccess

`AWSDataLifecycleManagerSSMFullAccess`ist eine AWSverwaltete Richtlinie, die: Amazon Data Lifecycle Manager die Erlaubnis erteilt, die Systems Manager Manager-Aktionen auszuführen, die für die Ausführung von Pre- und Post-Skripten auf allen Amazon EC2 EC2-Instances erforderlich sind.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataLifecycleManagerSSMFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 31. Oktober 2023, 20:29 UTC
- Bearbeitete Zeit: 16. November 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataPipeline_FullAccess

`AWSDataPipeline_FullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Data Pipeline, Listenzugriff für S3-, DynamoDB-, Redshift-, RDS-, SNS- und IAM-Rollen sowie PassRole-Zugriff für Standardrollen bietet.

Verwenden dieser -Richtlinie

Sie können`AWSDataPipeline_FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Januar 2017, 23:14 UTC
- Bearbeitete Zeit: 17. August 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataPipeline_PowerUser

`AWSDataPipeline_PowerUser`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Data Pipeline, Listenzugriff für S3-, DynamoDB-, Redshift-, RDS-, SNS- und IAM-Rollen sowie PassRole-Zugriff für Standardrollen bietet.

Verwenden dieser -Richtlinie

Sie können`AWSDataPipeline_PowerUser` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Januar 2017, 23:16 UTC
- Bearbeitete Zeit: 17. August 2017, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataSyncDiscoveryServiceRolePolicy

`AWSDataSyncDiscoveryServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: DataSync Discovery die Integration mit anderenAWS Diensten in Ihrem Namen ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 20. März 2023, 22:19 UTC
- Bearbeitete Zeit: 20. März 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtdokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataSyncFullAccess

`AWSDataSyncFullAccess` ist eine -AWS verwaltete Richtlinie, die: Vollzugriff auf AWS DataSync und minimalen Zugriff auf seine Abhängigkeiten bietet

Verwenden dieser Richtlinie

Sie können `AWSDataSyncFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2019, 19:40 UTC
- Bearbeitungszeit: 16. Februar 2024, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Richtlinienversion

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDataSyncReadOnlyAccess

`AWSDataSyncReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf gewährtAWS DataSync

Verwenden dieser -Richtlinie

Sie können`AWSDataSyncReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Januar 2019, 19:18 UTC
- Bearbeitete Zeit: 30. Juni 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeepLensLambdaFunctionAccessPolicy

`AWSDeepLensLambdaFunctionAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie spezifiziert die Berechtigungen, die für DeepLens administrative Lambda-Funktionen erforderlich sind, die auf einem DeepLens Gerät ausgeführt werden

Verwenden dieser -Richtlinie

Sie können`AWSDeepLensLambdaFunctionAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2017, 15:47 UTC
- Bearbeitete Zeit: 11. Juni 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeepLensServiceRolePolicy

`AWSDeepLensServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS DeepLens Zugriff auf Ressourcen und Rollen gewährtAWS-Services, die von DeepLens und deren Abhängigkeiten benötigt werden, einschließlich IoT, S3 GreenGrass undAWS Lambda.

Verwenden dieser Richtlinie

Sie können`AWSDeepLensServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 29. November 2017, 15:46 UTC
- Bearbeitete Zeit: 25. September 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion der -Standardrichtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeepRacerAccountAdminAccess

`AWSDeepRacerAccountAdminAccess`ist eine AWSverwaltete Richtlinie, die: DeepRacer Administratorzugriff auf alle Aktionen, einschließlich des Umschaltens zwischen Mehrbenutzer- und Einzelbenutzermodus.

Verwenden dieser -Richtlinie

Sie können`AWSDeepRacerAccountAdminAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. Oktober 2021, 01:27 UTC
- Bearbeitete Zeit: 28. Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete - Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeepRacerCloudFormationAccessPolicy

`AWSDeepRacerCloudFormationAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Es CloudFormation ermöglicht,AWS Stacks und Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

Verwenden dieser -Richtlinie

Sie könnenAWSDeepRacerCloudFormationAccessPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. Februar 2019, 21:59 UTC
- Bearbeitete Zeit: 14. Juni 2019, 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeepRacerDefaultMultiUserAccess

`AWSDeepRacerDefaultMultiUserAccess`ist eine AWSverwaltete Richtlinie, die: DeepRacer MultiUser Standardbenutzerzugriff zur Verwendung von Deepracer im Mehrbenutzermodus

Verwenden von dieser -Richtlinie

Sie können`AWSDeepRacerDefaultMultiUserAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. Oktober 2021, 01:27 UTC

- Bearbeitete Zeit: 28. Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen von -Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AWSDeepRacerFullAccess

`AWSDeepRacerFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf bietetAWS DeepRacer. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3).

Verwenden dieser -Richtlinie

Sie können`AWSDeepRacerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. Oktober 2020, 22:03 UTC
- Bearbeitete Zeit: 5. Oktober 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeepRacerRoboMakerAccessPolicy

`AWSDeepRacerRoboMakerAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Es ermöglicht RoboMaker , die erforderlichen Ressourcen zu erstellen undAWS Dienste in Ihrem Namen anzurufen.

Verwenden dieser Richtlinien

Sie könnenAWSDeepRacerRoboMakerAccessPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. Februar 2019, 21:59 UTC
- Bearbeitete Zeit: 28. Februar 2019, 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONRichtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeepRacerServiceRolePolicy

`AWSDeepRacerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es ermöglicht DeepRacer , die erforderlichen Ressourcen zu erstellen undAWS Dienste in Ihrem Namen anzurufen.

Verwenden von dieser -Richtlinie

Sie können`AWSDeepRacerServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 28. Februar 2019, 21:58 UTC

- Bearbeitete Zeit: 12. Juni 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von von von von von von von von von von von
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDenyAll

`AWSDenyAll`ist eine AWSverwaltete Richtlinie, die: jeglichen Zugriff verweigern.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDenyAll` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Mai 2019, 22:36 UTC
- Bearbeitete Zeit: 18. Dezember 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeviceFarmFullAccess

`AWSDeviceFarmFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alleAWS Device Farm Farm-Operationen bietet.

Verwenden dieser -Richtlinie

Sie könnenAWSDeviceFarmFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 13. Juli 2015, 16:37 UTC
- Bearbeitete Zeit: 13. Juli 2015, 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeviceFarmServiceRolePolicy

`AWSDeviceFarmServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Device Farm Berechtigungen zum Aufrufen von EC2-Netzwerk-APIs in Ihrem Namen gewähren.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 20. September 2022, 21:02 UTC
- Bearbeitete Zeit: 20. September 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDeviceFarmTestGridServiceRolePolicy

`AWSDeviceFarmTestGridServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Device Farm Berechtigungen zum Aufrufen von EC2-APIs in Ihrem Namen gewähren.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. Mai 2021, 22:01 UTC
- Bearbeitete Zeit: 26. Mai 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Direct Connect über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AWSDirectConnectFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 30. April 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
```

```
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDirectConnectReadOnlyAccess

`AWSDirectConnectReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff aufAWS Direct Connect über dieAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AWSDirectConnectReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 18. Mai 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie mit den geringsten Berechtigungen für die -Richtlinie festgelegt. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen für die geringste Anzahl von
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS den geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AWSDirectConnectServiceRolePolicy

`AWSDirectConnectServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Direct Connect die Berechtigung erteilt,AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 14. Januar 2021, 18:35 UTC
- Bearbeitete Zeit: 14. Januar 2021, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDirectoryServiceFullAccess

`AWSDirectoryServiceFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf denAWS Directory Service bietet.

Verwenden dieser Richtlinie

Sie können`AWSDirectoryServiceFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 24. November 2020, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Standardrichtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
    },
    {
      "Action" : [
```

```
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ds.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDirectoryServiceReadOnlyAccess

`AWSDirectoryServiceReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf denAWS Directory Service gewährt.

Verwenden dieser Richtlinie

Sie könnenAWSDirectoryServiceReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 25. September 2018, 21:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AWSDiscoveryContinuousExportFirehosePolicy

`AWSDiscoveryContinuousExportFirehosePolicy`ist eine AWSverwaltete Richtlinie, die: Schreibzugriff aufAWS Ressourcen gewährt, die fürAWS Discovery Continuous Export erforderlich sind

Verwenden dieser -Richtlinie

Sie können`AWSDiscoveryContinuousExportFirehosePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. August 2018, 18:29 UTC
- Bearbeitete Zeit: 8. Juni 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -die -die -die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDMSFleetAdvisorServiceRolePolicy

`AWSDMSFleetAdvisorServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es DMS Fleet Advisor ermöglicht, CloudWatch Kennzahlen in Ihrem Namen zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 6. März 2023, 09:10 UTC
- Bearbeitete Zeit: 06. März 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS

Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richt-Richt-

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSDMSServerlessServiceRolePolicy

`AWSDMSServerlessServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: AWS DMS Serverless Berechtigungen gewährt, um DMS-Ressourcen in Ihrem Konto in Ihrem Namen zu erstellen und zu verwalten

Verwenden von IAM-Richtlinien

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstverknüpfte Rollen
- Erstellungszeit: 18. Mai 2023
- Bearbeitete Zeit: 18. Mai 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-----

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
```

```
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:DeleteReplicationInstance"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mit AWS verwaltete Richtlinie und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSEC2CapacityReservationFleetRolePolicy

`AWSEC2CapacityReservationFleetRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es dem EC2 CapacityReservation Fleet Service ermöglicht, Kapazitätsreservierungen zu verwalten

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die CodeServicerolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 29. September 2021, 14:43 UTC
- Bearbeitete Zeit: 29. September 2021, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSEC2FleetServiceRolePolicy

`AWSEC2FleetServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es EC2 Fleet ermöglicht, Instances zu starten und zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. März 2018, 00:08 UTC
- Bearbeitete Zeit: 4. Mai 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSEC2SpotFleetServiceRolePolicy

`AWSEC2SpotFleetServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EC2 Spot Fleet den Start und die Verwaltung von Spot-Flotteninstanzen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die die die die die die die die die die die die die die die die die die die die die die die die die die Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 23. Oktober 2017, 19:13 UTC
- Bearbeitete Zeit: 16. März 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSEC2SpotServiceRolePolicy

`AWSEC2SpotServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EC2 Spot das Starten und Verwalten von Spot-Instances ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. September 2017, 18:51 UTC
- Bearbeitete Zeit: 12. Dezember 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSECRPullThroughCache_ServiceRolePolicy

`AWSECRPullThroughCache_ServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf AWS Dienste und Ressourcen ermöglicht, die vom AWS ECR-Pull-Through-Cache verwendet oder verwaltet werden

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2021, 21:51 UTC
- Bearbeitete Zeit: 13. November 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkCustomPlatformforEC2Role

`AWSElasticBeanstalkCustomPlatformforEC2Role`ist eine AWSverwaltete Richtlinie, die: der Instance in Ihrer benutzerdefinierten Platform Builder-Umgebung die Berechtigung zum Starten einer EC2-Instance, zum Erstellen von EBS-Snapshot und AMI, zum Streamen von Protokollen zu Amazon CloudWatch Logs und zum Speichern von Artefakten in Amazon S3 erteilt.

Verwenden dieser Richtlinie

Sie könnenAWSElasticBeanstalkCustomPlatformforEC2Role an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. Februar 2017, 22:50 UTC
- Bearbeitete Zeit: 21. Februar 2017, 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSElasticBeanstalkEnhancedHealth

`AWSElasticBeanstalkEnhancedHealth`ist eine AWSverwaltete Richtlinie, die:AWS Elastic Beanstalk Service-Richtlinie für das Health Monitoring-System

Verwenden dieser Richtlinie

Sie können`AWSElasticBeanstalkEnhancedHealth` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 8. Februar 2016, 23:17 UTC
- Bearbeitete Zeit: 9. April 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkMaintenance

`AWSElasticBeanstalkMaintenance`ist eine AWSverwaltete Richtlinie, die:AWS Elastic Beanstalk Service Role Policy, die eingeschränkte Berechtigungen gewährt, Ihre Ressourcen in Ihrem Namen zu Wartungszwecken zu aktualisieren.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 11. Januar 2019, 23:22 UTC
- Bearbeitete Zeit: 4. Juni 2019, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS

Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gilt für dieAWS Elastic Beanstalk-Servicerolle, mit der verwaltete Updates von Elastic Beanstalk Beanstalk-Umgebungen durchgeführt werden. Diese Richtlinie sollte nicht an andere Benutzer oder Rollen geknüpft werden. Die Richtlinie gewährt umfassende Berechtigungen zur Erstellung und Verwaltung von Ressourcen für eine Reihe vonAWS Diensten AutoScaling, darunter EC2, ECS, Elastic Load Balancing und CloudFormation. Diese Richtlinie ermöglicht auch die Weitergabe jeder IAM-Rolle, die für diese Dienste verwendet werden kann.

Verwenden dieser Richtlinie

Sie können`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. März 2021, 22:18 UTC
- Bearbeitete Zeit: 23. März 2023, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Standardversion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Elastic Beanstalk Service Role Policy, die eingeschränkte Berechtigungen für verwaltete Updates gewährt.

Verwenden von von von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an eine servicegebundene Rolle anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. November 2019, 22:35 UTC
- Bearbeitete Zeit: 24. März 2023, 00:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
```

```
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
```

```
    {
      "Sid" : "CWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
    },
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
```

```
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit vonAWS verwaltete

AWSElasticBeanstalkMulticontainerDocker

`AWSElasticBeanstalkMulticontainerDocker`ist eine AWSverwaltete Richtlinie, die: den Instances in Ihrer Multicontainer-Docker-Umgebung Zugriff gewähren, um den Amazon EC2 Container Service zur Verwaltung von Container-Bereitstellungsaufgaben zu verwenden.

Verwenden dieser Richtlinie

Sie könnenAWSElasticBeanstalkMulticontainerDocker an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Februar 2016, 23:15 UTC
- Bearbeitete Zeit: 23. März 2023, 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS mit den geringsten Richtlinien und Umstellung auf Berechtigungen

AWSElasticBeanstalkReadOnly

`AWSElasticBeanstalkReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Leserechte gewährt. Ermöglicht Operatoren ausdrücklich den direkten Zugriff auf Informationen über Ressourcen im Zusammenhang mitAWS Elastic Beanstalk Beanstalk-Anwendungen.

Verwenden dieser -Richtlinie

Sie können`AWSElasticBeanstalkReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. Januar 2021, 19:02 UTC
- Bearbeitete Zeit: 22. Januar 2021, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkRoleCore

`AWSElasticBeanstalkRoleCore`ist eine AWSverwaltete Richtlinie, die: AWSElasticBeanstalkRoleCore (Elastic Beanstalk Beanstalk-Betriebsrolle) Ermöglicht den Kernbetrieb einer Webservice-Umgebung.

Verwenden dieser Richtlinie

Sie können`AWSElasticBeanstalkRoleCore` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 5. Juni 2020, 21:48 UTC
- Bearbeitete Zeit: 9. September 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
```

```
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
      "Resource" : [
```

```
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*/*",
        "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
      ]
    },
```

```
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CancelUpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing:Delete*",
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
```

```
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
      ]
    },
    {
      "Sid" : "ListAPIs",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "logs:Describe*",
        "ec2:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticloadbalancing:Describe*",
        "rds:Describe*",
        "sns:List*",
        "iam:List*",
        "acm:Describe*",
        "acm:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
```

```
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkRoleCWL

`AWSElasticBeanstalkRoleCWL`List eine AWSverwaltete Richtlinie, die: (Elastic Beanstalk Beanstalk-Betriebsrolle) Es einer Umgebung ermöglicht, Amazon CloudWatch Log-Gruppen zu verwalten.

Verwenden dieser -Richtlinie

Sie können`AWSElasticBeanstalkRoleCWL` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 5. Juni 2020, 21:49 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSElasticBeanstalkRoleECS

`AWSElasticBeanstalkRoleECS`ist eine AWSverwaltete Richtlinie, die: (Elastic Beanstalk Beanstalk-Betriebsrolle) Ermöglicht es einer Docker-Umgebung mit mehreren Containern, Amazon ECS-Cluster zu verwalten.

Verwenden dieser -Richtlinie

Sie könnenAWSElasticBeanstalkRoleECS an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 5. Juni 2020, 21:47 UTC
- Bearbeitete Zeit: 23. März 2023, 22:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Berechtigungen. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkRoleRDS

`AWSElasticBeanstalkRoleRDS`ist eine AWSverwaltete Richtlinie, die: (Elastic Beanstalk Beanstalk-Betriebsrolle) Es einer Umgebung ermöglicht, eine Amazon RDS-Instance zu integrieren.

Verwenden dieser -Richtlinie

Sie können`AWSElasticBeanstalkRoleRDS` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 5. Juni 2020, 21:46 UTC

- Bearbeitete Zeit: 5. Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert Berechtigungen für die -Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien

AWSElasticBeanstalkRoleSNS

`AWSElasticBeanstalkRoleSNS`ist eine AWSverwaltete Richtlinie, die: (Elastic Beanstalk Beanstalk-Betriebsrolle) Es einer Umgebung ermöglicht, die Amazon SNS SNS-Themenintegration zu aktivieren.

Verwenden dieser -Richtlinie

Sie können`AWSElasticBeanstalkRoleSNS` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 5. Juni 2020, 21:46 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkRoleWorkerTier

`AWSElasticBeanstalkRoleWorkerTier`ist eine AWSverwaltete Richtlinie, die: (Elastic Beanstalk Beanstalk-Betriebsrolle) Ermöglicht es einer Ebene der Arbeitsumgebung, eine Amazon DynamoDB-Tabelle und eine Amazon SQS SQS-Warteschlange zu erstellen.

Verwenden dieser -Richtlinie

Sie können`AWSElasticBeanstalkRoleWorkerTier` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 5. Juni 2020, 21:43 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkService

`AWSElasticBeanstalkService`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist veraltet. Eine Anleitung finden Sie in der Dokumentation: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html. AWS Elastic Beanstalk Service-Rollenrichtlinie, die Berechtigungen zum Erstellen und Verwalten von Ressourcen (d. h.:AutoScaling EC2, S3CloudFormation, ELB usw.) in Ihrem Namen gewährt.

Verwenden von IAM-Richtlinie mit dieser

Sie können`AWSElasticBeanstalkService` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 11. April 2016, 20:27 UTC
- Bearbeitete Zeit: 10. Mai 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Version der Richtlinie

Version der Richtlinie:v17 (Standard)

Die Standardversion der Richtlinie definiert die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JAM-Richtlinie von JAM-Richtlinie

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von IAM-Richtlinie IAM-Richtlinie für IAM-Richtlinie IAM-Richtlinie
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinie und Umstellung auf Berechtigungen mit den geringsten sten sten ste verwaltete Richtlinie mit den geringsten sten ste

AWSElasticBeanstalkServiceRolePolicy

`AWSElasticBeanstalkServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Elastic Beanstalk Service Linked Role Policy AutoScaling, die Berechtigungen zum Erstellen und Verwalten von Ressourcen (d. h.: EC2 CloudFormation, S3, ELB usw.) in Ihrem Namen gewährt.

Verwenden von dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 13. September 2017, 23:46 UTC

- Bearbeitete Zeit: 06. Juni 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die StandardVersion ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

RichtRichtRichtRichtRichtRichtRicht

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkWebTier

`AWSElasticBeanstalkWebTier`ist eine AWSverwaltete Richtlinie, die: den Instances in Ihrer Webserverumgebung Zugriff zum Hochladen von Protokolldateien auf Amazon S3 gewähren.

Verwenden dieser -Richtlinie

Sie könnenAWSElasticBeanstalkWebTier an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Februar 2016, 23:08 UTC
- Bearbeitete Zeit: 9. September 2020, 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticBeanstalkWorkerTier

`AWSElasticBeanstalkWorkerTier`ist eine AWSverwaltete Richtlinie, die: den Instances in Ihrer Arbeitsumgebung Zugriff zum Hochladen von Protokolldateien auf Amazon S3 gewähren, Amazon SQS zur Überwachung der Auftragswarteschleife Ihrer Bewerbung verwenden, Amazon DynamoDB für die Wahl von Führungskräften verwenden und Amazon CloudWatch zur Veröffentlichung von Kennzahlen für die Gesundheitsüberwachung.

Verwenden dieser Richtlinien

Sie können`AWSElasticBeanstalkWorkerTier` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Februar 2016, 23:12 UTC
- Bearbeitete Zeit: 9. September 2020, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticDisasterRecoveryAgentInstallationPolicy

`AWSElasticDisasterRecoveryAgentInstallationPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Installation des AWS Replication Agents, der zusammen mit AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung externer Server verwendet wirdAWS. Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu, deren Anmeldeinformationen Sie bei der Installation des AWS Replication Agent angeben.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryAgentInstallationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:37 UTC
- Bearbeitete Zeit: 27. November 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryAgentPolicy

`AWSElasticDisasterRecoveryAgentPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Verwendung des AWS Replication Agents, der zusammen mit AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung von Quellservern verwendet wirdAWS. Es wird nicht empfohlen, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryAgentPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:32 UTC

- Bearbeitete Zeit: 27. November 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConsoleFullAccess

`AWSElasticDisasterRecoveryConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie bietet vollen Zugriff auf alle öffentlichen APIs von AWS Elastic Disaster Recovery (DRS) sowie Berechtigungen zum Lesen von KMS-Schlüsseln, License Manager, Resource Groups, Elastic Load Balancing, IAM- und EC2-Informationen. Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:46 UTC
- Bearbeitete Zeit: 16. Oktober 2023, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConsoleFullAccess_v2

`AWSElasticDisasterRecoveryConsoleFullAccess_v2`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie bietet vollen Zugriff auf alle öffentlichen APIs von AWS Elastic Disaster Recovery (AWSDRS) sowie auf alle öffentlichen APIs in anderen AWS Services, die von der AWS DRS-Konsole verwendet werden. Fügen Sie diese Richtlinie Ihren Benutzern oder Rollen hinzu.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryConsoleFullAccess_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2023, 13:35 UTC
- Bearbeitete Zeit: 27. November 2023, 13:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConversionServerPolicy

`AWSElasticDisasterRecoveryConversionServerPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist der Instanzrolle des AWS Elastic Disaster Recovery Conversion-Servers zugeordnet. Diese Richtlinie ermöglicht es Elastic Disaster Recovery (DRS) -Konversionsservern, bei denen es sich um EC2-Instances handelt, die von Elastic Disaster Recovery gestartet wurden, mit dem DRS-Service zu kommunizieren. Eine IAM-Rolle mit dieser Richtlinie wird von DRS (als EC2-Instance-Profil) an die DRS-Konvertierungsserver angehängt, die bei Bedarf automatisch von DRS gestartet und beendet werden. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen. DRS-Konvertierungsserver werden von Elastic Disaster Recovery verwendet, wenn Benutzer Quellserver mithilfe der DRS-Konsole, CLI oder API wiederherstellen möchten.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryConversionServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 13:42 UTC
- Bearbeitete Zeit: 27. November 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` ist eine von AWS verwaltete Richtlinie, die: Diese Richtlinie ermöglicht AWS Elastic Disaster Recovery (DRS), die kontoübergreifende Replikation und kontoübergreifendes Failback zu unterstützen.

Verwenden dieser Richtlinie

Sie können `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 14. Mai 2023, 07:16 UTC
- Bearbeitungszeit: 17. Januar 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryEc2InstancePolicy

`AWSElasticDisasterRecoveryEc2InstancePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS Replication Agents, der von AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung von Quellservern verwendet wird, die auf EC2 laufen (regionsübergreifend oder azübergreifend). Eine IAM-Rolle mit dieser Richtlinie sollte (als EC2-Instance-Profil) an die EC2-Instances angehängt werden.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryEc2InstancePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Mai 2022, 12:30 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryFailbackInstallationPolicy

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`ist eine AWSverwaltete Richtlinie, die: Sie können die AWSElasticDisasterRecoveryFailbackInstallationPolicy Richtlinie an Ihre IAM-Identitäten anhängen. Diese Richtlinie ermöglicht die Installation des Elastic Disaster Recovery Failback Client, der für ein Failback von Wiederherstellungsinstanzen auf Ihre ursprüngliche Quellinfrastruktur verwendet wird. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu, deren Anmeldeinformationen Sie bei der Ausführung des Elastic Disaster Recovery Failback Client angeben.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryFailbackInstallationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 11:02 UTC
- Bearbeitete Zeit: 27. November 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryFailbackPolicy

`AWSElasticDisasterRecoveryFailbackPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht die Verwendung des Elastic Disaster Recovery Failback Client, der für ein Failback von Wiederherstellungsinstanzen auf Ihre ursprüngliche Quellinfrastruktur verwendet wird. Wir empfehlen nicht, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryFailbackPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:41 UTC
- Bearbeitete Zeit: 27. November 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryLaunchActionsPolicy

`AWSElasticDisasterRecoveryLaunchActionsPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es Ihnen, Amazon SSM und weitere für Dienste erforderliche Berechtigungen zu verwenden, um Aktionen nach dem Start in AWS Elastic Disaster Recovery (AWSDRS) auszuführen. Fügen Sie diese Richtlinie Ihren IAM-Rollen oder -Benutzern hinzu.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryLaunchActionsPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. September 2023, 07:38 UTC
- Bearbeitete Zeit: 16. Oktober 2023, 12:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryNetworkReplicationPolicy

`AWSElasticDisasterRecoveryNetworkReplicationPolicy` ist eine von AWS verwaltete Richtlinie, die: Diese Richtlinie ermöglicht AWS Elastic Disaster Recovery (DRS), die Netzwerkreplikation zu unterstützen.

Verwenden dieser Richtlinie

Sie können `AWSElasticDisasterRecoveryNetworkReplicationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 11. Juni 2023, 12:36 UTC
- Bearbeitungszeit: 02. Januar 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Richtlinienversion

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryReadOnlyAccess

`AWSElasticDisasterRecoveryReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die:
Sie können die AWSElasticDisasterRecoveryReadOnlyAccess Richtlinie an Ihre IAM-Identitäten anhängen. Diese Richtlinie gewährt Berechtigungen für alle schreibgeschützten öffentlichen APIs von Elastic Disaster Recovery (DRS) sowie für einige schreibgeschützte APIs anderer AWS Dienste, die erforderlich sind, um die DRS-Konsole vollständig schreibgeschützt nutzen zu können. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:50 UTC
- Bearbeitete Zeit: 27. November 2023, 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryRecoveryInstancePolicy

`AWSElasticDisasterRecoveryRecoveryInstancePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist der Instanzrolle der Wiederherstellungsinstanz von Elastic Disaster Recovery zugeordnet. Diese Richtlinie ermöglicht es der Elastic Disaster Recovery (DRS) Recovery Instance, bei der es sich um EC2-Instances handelt, die von Elastic Disaster Recovery gestartet wurden, mit dem DRS-Service zu kommunizieren und auf ihre ursprüngliche Quellinfrastruktur zurückzugreifen. Eine IAM-Rolle mit dieser Richtlinie wird (als EC2-Instance-Profil) von Elastic Disaster Recovery den DRS-Wiederherstellungsinstanzen zugewiesen. Wir empfehlen nicht, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryRecoveryInstancePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:20 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryReplicationServerPolicy

`AWSElasticDisasterRecoveryReplicationServerPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist an die Instanzrolle des Elastic Disaster Recovery Replication-Servers angehängt. Diese Richtlinie ermöglicht es den Elastic Disaster Recovery (DRS) Replication Servern, bei denen es sich um EC2-Instances handelt, die von Elastic Disaster Recovery gestartet wurden, mit dem DRS-Service zu kommunizieren und EBS-Snapshots in Ihrem zu erstellen. AWS-Konto Eine IAM-Rolle mit dieser Richtlinie wird (als EC2-Instance-Profil) von Elastic Disaster Recovery den DRS-Replikationsservern zugewiesen, die bei Bedarf automatisch von DRS gestartet und beendet werden. DRS-Replikationsserver werden verwendet, um die Datenreplikation von Ihren externen Servern auf die AWS Daten als Teil des von DRS verwalteten Wiederherstellungsprozesses zu erleichtern. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryReplicationServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 13:34 UTC
- Bearbeitete Zeit: 27. November 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryServiceRolePolicy

`AWSElasticDisasterRecoveryServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Diese Richtlinie ermöglicht Elastic Disaster Recovery, -AWSRessourcen in Ihrem Namen zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 17. November 2021, 10:56 UTC
- Bearbeitungszeit: 17. Januar 2024, 13:49 UTC

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

Richtlinienversion

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryStagingAccountPolicy

`AWSElasticDisasterRecoveryStagingAccountPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht den schreibgeschützten Zugriff auf AWS Elastic Disaster Recovery (DRS) -Ressourcen wie Quellserver und Jobs. Sie ermöglicht auch die Erstellung eines konvertierten Snapshots und die gemeinsame Nutzung dieses EBS-Snapshots mit einem bestimmten Konto.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryStagingAccountPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Mai 2022, 09:49 UTC
- Bearbeitete Zeit: 27. November 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie wird von AWS Elastic Disaster Recovery (DRS) verwendet, um Quellserver

in einem separaten Zielkonto wiederherzustellen und ein Failback zu ermöglichen. Es wird nicht empfohlen, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Januar 2023, 12:11 UTC
- Bearbeitete Zeit: 27. November 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticLoadBalancingClassicServiceRolePolicy

`AWSElasticLoadBalancingClassicServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Service Linked Role Policy fürAWS Elastic Load Balancing Control Plane — Classic

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. September 2017, 22:36 UTC
- Bearbeitete Zeit: 7. Oktober 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie definiert, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElasticLoadBalancingServiceRolePolicy

`AWSElasticLoadBalancingServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Service Linked Role Policy forAWS Elastic Load Balancing Control Plane

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. September 2017, 22:19 UTC
- Bearbeitete Zeit: 26. August 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die StandardRichtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtloy ermöglicht

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElementalMediaConvertFullAccess

`AWSElementalMediaConvertFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Elemental MediaConvert über dasAWS Management Console und SDK bietet.

Verwenden dieser -Richtlinie

Sie können`AWSElementalMediaConvertFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. Juni 2018, 19:25 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElementalMediaConvertReadOnly

`AWSElementalMediaConvertReadOnly`ist eine AWSverwaltete Richtlinie, die: MediaConvert Über dasAWS Management Console und SDK nur Lesezugriff aufAWS Elemental bietet.

Verwenden dieser -Richtlinie

Sie können`AWSElementalMediaConvertReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. Juni 2018, 19:25 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElementalMediaLiveFullAccess

`AWSElementalMediaLiveFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS elementare MediaLive Ressourcen bietet

Verwenden dieser -Richtlinie

Sie könnenAWSElementalMediaLiveFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Juli 2020, 17:07 UTC
- Bearbeitete Zeit: 8. Juli 2020, 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElementalMediaLiveReadOnly

`AWSElementalMediaLiveReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS MediaLive Elementarressourcen gewährt

Verwenden dieser Richtlinie

Sie können`AWSElementalMediaLiveReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Juli 2020, 16:38 UTC
- Bearbeitete Zeit: 8. Juli 2020, 16:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion definiert die Berechtigungen für die -Standardrichtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "medialive:List*",
      "medialive:Describe*"
    ],
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElementalMediaPackageFullAccess

`AWSElementalMediaPackageFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS elementare MediaPackage Ressourcen bietet

Verwenden dieser -Richtlinie

Sie können`AWSElementalMediaPackageFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. Dezember 2017, 23:39 UTC
- Bearbeitete Zeit: 29. Dezember 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElementalMediaPackageReadOnly

`AWSElementalMediaPackageReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS MediaPackage Elementarressourcen gewährt

Verwenden dieser -Richtlinie

Sie können`AWSElementalMediaPackageReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. Dezember 2017, 00:04 UTC
- Bearbeitete Zeit: 30. Dezember 2017, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSElementalMediaPackageV2FullAccess

`AWSElementalMediaPackageV2FullAccess`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff aufAWSElementarMediaPackageV2-Ressourcen.

Verwendung dieser Richtlinie

Sie können anhängen`AWSElementalMediaPackageV2FullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 25. Juli 2023, 20:29 Uhr UTC
- Uhrzeit der Bearbeitung:25. Juli 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageV2ReadOnly

`AWSElementalMediaPackageV2ReadOnly`ist einAWSverwaltete Richtliniedas: Bietet schreibgeschützten Zugriff aufAWSElementarMediaPackageV2-Ressourcen.

Verwendung dieser Richtlinie

Sie können anhängen`AWSElementalMediaPackageV2ReadOnly`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 25. Juli 2023, 20:31 Uhr UTC
- Uhrzeit der Bearbeitung:25. Juli 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSElementalMediaStoreFullAccess

`AWSElementalMediaStoreFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Lese- und Schreibzugriff auf alle MediaStore APIs bietet

Verwenden dieser -Richtlinie

Sie können`AWSElementalMediaStoreFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. März 2018, 23:15 UTC
- Bearbeitete Zeit: 5. März 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElementalMediaStoreReadOnly

`AWSElementalMediaStoreReadOnly`ist eine AWSverwaltete Richtlinie, die: Schreibgeschützte Berechtigungen für MediaStore APIs bereitstellt

Verwenden dieser -Richtlinie

Sie können`AWSElementalMediaStoreReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 8. März 2018, 19:48 UTC
- Bearbeitete Zeit: 8. März 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien

AWSElementalMediaTailorFullAccess

`AWSElementalMediaTailorFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS elementare MediaTailor Ressourcen bietet

Verwenden dieser -Richtlinie

Sie können`AWSElementalMediaTailorFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. November 2021, 00:04 UTC
- Bearbeitete Zeit: 23. November 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSElementalMediaTailorReadOnly

`AWSElementalMediaTailorReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS MediaTailor Elementarressourcen gewährt

Verwenden dieser -Richtlinie

Sie können`AWSElementalMediaTailorReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. November 2021, 00:05 UTC
- Bearbeitete Zeit: 23. November 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSEnhancedClassicNetworkingMangementPolicy

`AWSEnhancedClassicNetworkingMangementPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung einer erweiterten klassischen Netzwerkverwaltungsfunktion.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 20. September 2017, 17:29 UTC
- Bearbeitete Zeit: 20. September 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version der Richtlinie, die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JRichtdokument JJJdokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSEntityResolutionConsoleFullAccess

`AWSEntityResolutionConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff über die Konsole auf AWS Entity Resolution und zugehörige Dienste gewährt.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSEntityResolutionConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. August 2023, 17:54 UTC
- Bearbeitete Zeit: 16. Oktober 2023, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEntityResolutionConsoleReadOnlyAccess

`AWSEntityResolutionConsoleReadOnlyAccess`ist einAWSverwaltete Richtliniedas: Bietet schreibgeschützten Zugriff aufAWSAuflösung von Entitäten überAWS Management Console.

Verwendung dieser Richtlinie

Sie können anhängen`AWSEntityResolutionConsoleReadOnlyAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie
- Zeitpunkt der Erstellung: 17. August 2023, 18:18 Uhr UTC
- Bearbeitete Zeit:17. August 2023, 18:18 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorEC2Access

`AWSFaultInjectionSimulatorEC2Access`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt dem Fault Injection Simulator Service in EC2 und anderen erforderlichen Diensten die Erlaubnis, FIS-Aktionen auszuführen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorEC2Access` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:39 UTC
- Bearbeitete Zeit: 27. November 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorECSAccess

`AWSFaultInjectionSimulatorECSAccess` ist eine -AWSverwaltete Richtlinie, die: Diese Richtlinie erteilt dem Fault Injection Simulator Service die Berechtigung in ECS und anderen erforderlichen Services, um FIS-Aktionen durchzuführen.

Verwenden dieser Richtlinie

Sie können `AWSFaultInjectionSimulatorECSAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 26. Oktober 2022, 20:37 UTC
- Bearbeitungszeit: 25. Januar 2024, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen

- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorEKSAccess

`AWSFaultInjectionSimulatorEKSAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie erteilt dem Fault Injection Simulator Service in EKS und anderen erforderlichen Diensten die Erlaubnis, FIS-Aktionen auszuführen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorEKSAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:34 UTC
- Bearbeitete Zeit: 13. November 2023, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorNetworkAccess

`AWSFaultInjectionSimulatorNetworkAccess` ist eine von AWS verwaltete Richtlinie, die: Diese Richtlinie erteilt dem Fault Injection Simulator Service die Berechtigung in EC2-Netzwerken und anderen erforderlichen Services, um FIS-Aktionen durchzuführen.

Verwenden dieser Richtlinie

Sie können `AWSFaultInjectionSimulatorNetworkAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 26. Oktober 2022, 20:32 UTC
- Bearbeitungszeit: 25. Januar 2024, 16:07 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorRDSAccess

`AWSFaultInjectionSimulatorRDSAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie erteilt dem Fault Injection Simulator Service in RDS und anderen erforderlichen Diensten die Erlaubnis, FIS-Aktionen auszuführen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorRDSAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:30 Uhr UTC
- Bearbeitete Zeit: 13. November 2023, 16:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorSSMAccess

`AWSFaultInjectionSimulatorSSMAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt dem Fault Injection Simulator Service die Berechtigung in SSM und anderen erforderlichen Diensten zur Durchführung von FIS-Aktionen.

Verwenden dieser -Richtlinie

Sie können Verbindungen `AWSFaultInjectionSimulatorSSMAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Dienstrollen
- Aufnahmezeit: 26. Oktober 2022, 15:33 UTC
- Bearbeitete Zeit: 02. Juni 2023, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSFinSpaceServiceRolePolicy

`AWSFinSpaceServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung des Zugriffs auf AWS-Service und Ressourcen, die von Amazon verwendet oder verwaltet werden FinSpace

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Mai 2023, 16:42 UTC
- Bearbeitete Zeit: 1. Dezember 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFMAdminFullAccess

`AWSFMAdminFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff fürAWS FM Administrator

Verwenden dieser -Richtlinie

Sie können`AWSFMAdminFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 9. Mai 2018, 18:06 UTC
- Bearbeitete Zeit: 20. Oktober 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSFMAdminReadOnlyAccess

`AWSFMAdminReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff für denAWS FM-Administrator, der die Überwachung desAWS FM-Betriebs ermöglicht

Verwenden dieser Richtlinie

Sie können`AWSFMAdminReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Mai 2018, 20:07 UTC
- Bearbeitete Zeit: 31. Oktober 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSFMMemberReadOnlyAccess

`AWSFMMemberReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS WAF-Aktionen fürAWS Firewall Manager Manager-Mitgliedskonten gewährt

Verwenden dieser -Richtlinie

Sie können`AWSFMMemberReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 9. Mai 2018, 21:05 UTC
- Bearbeitete Zeit: 9. Mai 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -verwaltete -verwaltete -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSForWordPressPluginPolicy

`AWSForWordPressPluginPolicy`ist eine AWSverwaltete Richtlinie, die: Verwaltete Richtlinie für dasAWS For Wordpress Plugin

Verwenden dieser -Richtlinie

Sie können`AWSForWordPressPluginPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. Oktober 2019, 00:27 UTC
- Bearbeitete Zeit: 20. Januar 2020, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGitSyncServiceRolePolicy

`AWSGitSyncServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die es AWS Code Connections ermöglicht, Inhalte aus Ihrem Git-Repository zu synchronisieren

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. November 2023, 17:05 UTC
- Bearbeitete Zeit: 16. November 2023, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlobalAcceleratorSLRPolicy

`AWSGlobalAcceleratorSLRPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die AWS Global Accelerator Berechtigungen zur Verwaltung von EC2 Elastic Network Interfaces und Security Groups gewährt.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. April 2019, 19:39 UTC
- Bearbeitete Zeit: 12. September 2023, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueConsoleFullAccess

`AWSGlueConsoleFullAccess`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff aufAWSKleben Sie über denAWS Management Console

Verwendung dieser Richtlinie

Sie können anhängen`AWSGlueConsoleFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 14. August 2017, 13:37 Uhr UTC
- Uhrzeit der Bearbeitung:14. Juli 2023, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie: v14(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSGlueConsoleSageMakerNotebookFullAccess

`AWSGlueConsoleSageMakerNotebookFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Glue über dieAWS Management Console und Zugriff auf Sagemaker-Notebook-Instanzen bietet.

Verwenden dieser Richtlinie

Sie könnenAWSGlueConsoleSageMakerNotebookFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. Oktober 2018, 17:52 UTC
- Bearbeitete Zeit: 15. Juli 2021, 15:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AwsGlueDataBrewFullAccessPolicy

`AwsGlueDataBrewFullAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Glue DataBrew über die bietetAWS Management Console. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, KMS, Glue).

Verwenden dieser -Richtlinie verwenden von -

Sie können`AwsGlueDataBrewFullAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. November 2020, 16:51 UTC
- Bearbeitete Zeit: 4. Februar 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von IAM-Identitätsberechtigungen und Hinzufügen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGlueDataBrewServiceRole

`AWSGlueDataBrewServiceRole` ist eine -AWS verwaltete Richtlinie, die: Diese Richtlinie gewährt Glue die Berechtigung, Aktionen im Glue-Datenkatalog des Benutzers auszuführen. Diese Richtlinie bietet auch die Berechtigung, ec2-Aktionen durchzuführen, damit Glue ENI erstellen kann, um eine Verbindung zu Ressourcen in der VPC herzustellen, und Glue auch den Zugriff auf registrierte Daten in Lakeformation und die Berechtigung auf die Cloudwatch des Benutzers zu ermöglichen.

Verwenden dieser Richtlinie

Sie können `AWSGlueDataBrewServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 04. Dezember 2020, 21:26 UTC
- Bearbeitungszeit: 20. März 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Richtlinienversion

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSGlueSchemaRegistryFullAccess

`AWSGlueSchemaRegistryFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf denAWS Glue Schema Registry Service bietet

Verwenden dieser Richtlinie

Sie können`AWSGlueSchemaRegistryFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2020, 00:19 UTC
- Bearbeitete Zeit: 20. November 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGlueSchemaRegistryReadonlyAccess

`AWSGlueSchemaRegistryReadonlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf denAWS Glue Schema Registry Service gewährt

Verwenden dieser -verwaltete

Sie könnenAWSGlueSchemaRegistryReadonlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. November 2020 00:20 UTC
- Bearbeitete Zeit: 20. November 2020, 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGlueServiceNotebookRole

`AWSGlueServiceNotebookRole`ist eine AWSverwaltete Richtlinie, die: Richtlinie für die AWS Glue-Servicerolle, die es dem Kunden ermöglicht, den Notebook-Server zu verwalten

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueServiceNotebookRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:37 UTC
- Bearbeitete Zeit: 9. Oktober 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueServiceRole

`AWSGlueServiceRole`ist eine AWSverwaltete Richtlinie, die: Richtlinie für die AWS Glue-Dienstrolle, die den Zugriff auf verwandte Dienste wie EC2, S3 und Cloudwatch Logs ermöglicht

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:37 Uhr UTC

- Bearbeitete Zeit: 11. September 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedNotebookPolicy

`AwsGlueSessionUserRestrictedNotebookPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen bereitstellt, die es Benutzern ermöglichen, nur die Notizbuchsitzungen zu erstellen und zu verwenden, die dem Benutzer zugeordnet sind. Diese Richtlinie beinhaltet auch Berechtigungen, die es Benutzern ausdrücklich ermöglichen, eine eingeschränkte Glue-Sitzungsrolle zu übergeben.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AwsGlueSessionUserRestrictedNotebookPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. April 2022, 15:24 UTC
- Bearbeitete Zeit: 22. November 2023, 01:32 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedNotebookServiceRole

`AwsGlueSessionUserRestrictedNotebookServiceRole`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alleAWS Glue-Ressourcen mit Ausnahme von Glue-Ressourcen enthält. Ermöglicht Benutzern, nur die Notebook-Sitzungen zu erstellen und zu verwenden, die mit dem Benutzer verknüpft sind. Diese Richtlinie enthält auch andere Berechtigungen, die vonAWS Glue benötigt werden, um Glue-Ressourcen in anderenAWS -Services zu verwalten.

Verwenden dieser Richtlinie

Sie können`AwsGlueSessionUserRestrictedNotebookServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 18. April 2022, 15:27 UTC
- Bearbeitete Zeit: 18. April 2022, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie enthält die die die die die die die die die die die die Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONRichtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AwsGlueSessionUserRestrictedPolicy

`AwsGlueSessionUserRestrictedPolicy`ist eine AWSverwaltete -Ressourcen, die Benutzern ermöglichen, interaktive Sitzungen zu erstellen und zu verwenden, die mit dem Benutzer verknüpft sind. Diese Richtlinie enthält auch Berechtigungen, die Benutzern ermöglichen, nur eine eingeschränkte Glue-Sitzungsrolle zu verwenden.

Verwenden dieser Richtlinie

Sie können`AwsGlueSessionUserRestrictedPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. April 2022, 21:31 UTC
- Bearbeitete Zeit: 14. April 2022, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Berechtigungen definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-JSON-Richtlinie

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

```
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
```

```
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AwsGlueSessionUserRestrictedServiceRole

`AwsGlueSessionUserRestrictedServiceRole`ist eine AWS-verwaltete Richtlinie enthält vollständigen Zugriff auf alleAWS Glue -Ressourcen außer Sitzungen. Ermöglicht Benutzern, nur die interaktiven Sitzungen zu erstellen und zu verwenden, die mit dem Benutzer verknüpft sind. Diese Richtlinie enthält auch andere Berechtigungen, die vonAWS Glue benötigt werden, um Glue -Ressourcen in anderenAWS -Services zu verwalten.

Verwenden dieser Richtlinie Richtlinie Richtlinie Richtlinie enthält

Sie können`AwsGlueSessionUserRestrictedServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. April 2022, 21:30 UTC
- Bearbeitete Zeit: 14. April 2022, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument dokument

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

```
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
```

```
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
```

```
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGrafanaAccountAdministrator

`AWSGrafanaAccountAdministrator`ist eine AWSverwaltete Richtlinie, die: Zugriff innerhalb von Amazon Grafana ermöglicht, um Arbeitsbereiche für die gesamte Organisation zu erstellen und zu verwalten.

Verwenden dieser -Richtlinie

Sie können`AWSGrafanaAccountAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. Februar 2021, 00:20 UTC
- Bearbeitete Zeit: 15. Februar 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGrafanaConsoleReadOnlyAccess

`AWSGrafanaConsoleReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf schreibgeschützten Operationen in Amazon Grafana.

Verwenden dieser -Richtlinie

Sie können`AWSGrafanaConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 23. Februar 2021, 00:10 UTC
- Bearbeitete Zeit: 15. Februar 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSGrafanaWorkspacePermissionManagement

`AWSGrafanaWorkspacePermissionManagement`ist eine AWSverwaltete Richtlinie, die: Nur die Möglichkeit bietet, Benutzer- und Gruppenberechtigungen fürAWS Grafana-Arbeitsbereiche zu aktualisieren.

Verwenden dieser Richtlinie

Sie können`AWSGrafanaWorkspacePermissionManagement` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. Februar 2021, 00:15 UTC
- Bearbeitete Zeit: 15. März 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGrafanaWorkspacePermissionManagementV2

`AWSGrafanaWorkspacePermissionManagementV2` ist eine von AWS verwaltete Richtlinie, die: Ermöglicht, IAM Identity Center (IdC)-Benutzer- und Gruppenberechtigungen für Amazon Managed Grafana Workspaces zu aktualisieren.

Verwenden dieser Richtlinie

Sie können `AWSGrafanaWorkspacePermissionManagementV2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 05. Januar 2024, 18:39 UTC
- Bearbeitungszeit: 05. Januar 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSGreengrassFullAccess

`AWSGreengrassFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt vollen Zugriff auf die Konfigurations-, Verwaltungs- und Bereitstellungsmaßnahmen vonAWS Greengrass

Verwenden dieser -Richtlinie

Sie können`AWSGreengrassFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 3. Mai 2017 00:47 UTC
- Bearbeitete Zeit: 3. Mai 2017, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-AM-AM-AM-AM-AM-AM-AM-AM-AM-
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGreengrassReadOnlyAccess

`AWSGreengrassReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt nur Lesezugriff auf die Konfigurations-, Management- und Bereitstellungsaktionen vonAWS Greengrass

Verwenden dieser -Richtlinie

Sie können`AWSGreengrassReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. Oktober 2018, 16:01 UTC
- Bearbeitete Zeit: 30. Oktober 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGreengrassResourceAccessRolePolicy

`AWSGreengrassResourceAccessRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie für dieAWS Greengrass-Servicerolle, die den Zugriff auf verwandte Dienste wieAWS Lambda- undAWS IoT-Shadows ermöglicht.

Verwenden dieser -Richtlinie

Sie können`AWSGreengrassResourceAccessRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. Februar 2017 21:17 UTC
- Bearbeitete Zeit: 14. November 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete Version ist die -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSGroundStationAgentInstancePolicy

`AWSGroundStationAgentInstancePolicy`ist eine AWSverwaltete Richtlinie, die: Die Dataflow Endpoint-Instanzberechtigungen zur Verwendung desAWS Ground Station Agents bereitstellt

Verwenden dieser Richtlinien

Sie können`AWSGroundStationAgentInstancePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. März 2023, 15:23 UTC
- Bearbeitete Zeit: 29. März 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSHealth_EventProcessorServiceRolePolicy

`AWSHealth_EventProcessorServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Health ermöglicht, die Health Event Processor-Funktion zu aktivieren.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die servicegebundene Rolle angehängt, die die die die servicegebundene Rolle angehängt. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 13. Januar 2023, 19:24 UTC
- Bearbeitete Zeit: 13. Januar 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die die die Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf die geringsten Berechtigungen

AWSHealthFullAccess

`AWSHealthFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf dieAWS Health Apis und Benachrichtigungen sowie das Personal Health Dashboard ermöglicht

Verwenden dieser -Richtlinie

Sie können`AWSHealthFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Dezember 2016, 12:30 UTC
- Bearbeitete Zeit: 16. November 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON--Richtliniendokument

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSHealthImagingFullAccess

`AWSHealthImagingFullAccess`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff aufAWSService zur Bildgebung im Gesundheitswesen.

Verwendung dieser Richtlinie

Sie können anhängen`AWSHealthImagingFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Entstehungszeit: 25. Juli 2023, 23:39 Uhr UTC
- Uhrzeit der Bearbeitung:25. Juli 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eineAWSressource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSHealthImagingReadOnlyAccess

`AWSHealthImagingReadOnlyAccess`ist einAWSverwaltete Richtliniedas: Bietet nur Lesezugriff aufAWSService zur Bildgebung im Gesundheitswesen.

Verwendung dieser Richtlinie

Sie können anhängen`AWSHealthImagingReadOnlyAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 25. Juli 2023, 23:40 Uhr UTC
- Uhrzeit der Bearbeitung:01. August 2023, 15:18 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie: v2(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSIAMIdentityCenterAllowListForIdentityContext

`AWSIAMIdentityCenterAllowListForIdentityContext`ist eine AWSverwaltete Richtlinie, die: Die Liste der Aktionen enthält, die für Rollen zulässig sind, die im IAM Identity Center-Identitätskontext übernommen wurden. AWS Security Token Service (AWSSTS) ordnet diese Richtlinie automatisch den übernommenen Rollen zu. Der Identitätskontext wird als ProvidedContext übergeben.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSIAMIdentityCenterAllowListForIdentityContext` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 08. November 2023, 15:21 UTC
- Bearbeitete Zeit: 25. November 2023, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
```

```
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIdentitySyncFullAccess

`AWSIdentitySyncFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf den Identity Sync-Dienst gewährt

Verwenden dieser -Richtlinie

Sie können`AWSIdentitySyncFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. März 2022, 23:29 UTC
- Bearbeitete Zeit: 23. März 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIdentitySyncReadOnlyAccess

`AWSIdentitySyncReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf den Identity Sync-Dienst

Verwenden dieser -Richtlinie

Sie können`AWSIdentitySyncReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. März 2022, 23:29 UTC
- Bearbeitete Zeit: 23. März 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSImageBuilderFullAccess

`AWSImageBuilderFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf alleAWS Image Builder Builder-Aktionen und ressourcenspezifischen Zugriff auf zugehörigeAWS Dienste bietet.

Verwenden dieser -Richtlinie

Sie können`AWSImageBuilderFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. Dezember 2019, 18:25 UTC
- Bearbeitete Zeit: 13. April 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSImageBuilderReadOnlyAccess

`AWSImageBuilderReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf alleAWS Image Builder Builder-Aktionen gewährt.

Verwenden dieser -Richtlinie

Sie können`AWSImageBuilderReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Dezember 2019, 22:29 UTC

- Bearbeitete Zeit: 19. Dezember 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSImportExportFullAccess

`AWSImportExportFullAccess`ist eine AWSverwaltete Richtlinie, die: Lese- und Schreibzugriff auf die Jobs gewährt, die im Rahmen von erstellt wurdenAWS-Konto.

Verwenden dieser -Richtlinie

Sie können`AWSImportExportFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSImportExportReadOnlyAccess

`AWSImportExportReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf die Jobs gewährt, die im Rahmen von erstellt wurdenAWS-Konto.

Verwenden dieser -Richtlinie

Sie können`AWSImportExportReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIncidentManagerIncidentAccessServiceRolePolicy

`AWSIncidentManagerIncidentAccessServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Gewährt Incident Manager Berechtigungen zum Aufrufen anderer - AWS Services im Rahmen der Verwaltung eines Vorfalls.

Verwenden dieser Richtlinie

Sie können `AWSIncidentManagerIncidentAccessServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie

- Erstellungszeit: 13. November 2023, 00:01 UTC
- Bearbeitungszeit: 20. Februar 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIncidentManagerResolverAccess

`AWSIncidentManagerResolverAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen zum Starten, Anzeigen und Aktualisieren von Vorfällen mit vollem Zugriff auf benutzerdefinierte Timeline-Ereignisse und zugehörige Elemente. Weisen Sie diese Richtlinie Benutzern zu, die Vorfälle erstellen und lösen.

Verwenden dieser -Richtlinie

Sie können`AWSIncidentManagerResolverAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 10. Mai 2021, 06:12 UTC
- Bearbeitete Zeit: 10. Mai 2021, 06:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIncidentManagerServiceRolePolicy

`AWSIncidentManagerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie erteilt Incident Manager die Erlaubnis, die Aufzeichnungen über Vorfälle und zugehörige Ressourcen in Ihrem Namen zu verwalten.

von von von von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen angehängt haben.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 10. Mai 2021, 03:34 UTC
- Bearbeitete Zeit: 5. Dezember 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinien Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinien

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoT1ClickFullAccess

`AWSIoT1ClickFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS IoT 1-Click bietet.

Verwenden dieser -Richtlinie

Sie können`AWSIoT1ClickFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Mai 2018, 22:10 UTC
- Bearbeitete Zeit: 11. Mai 2018, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSIoT1ClickReadOnlyAccess

`AWSIoT1ClickReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS IoT 1-Click bietet.

Verwenden dieser -Richtlinie

Sie können`AWSIoT1ClickReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Mai 2018 21:49 UTC
- Bearbeitete Zeit: 11. Mai 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTAnalyticsFullAccess

`AWSIoTAnalyticsFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf IoT Analytics bietet.

Verwenden dieser -Richtlinie

Sie können`AWSIoTAnalyticsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Juni 2018, 23:02 UTC

- Bearbeitete Zeit: 18. Juni 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTAnalyticsReadOnlyAccess

`AWSIoTAnalyticsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf IoT Analytics bietet.

Verwenden dieser Richtlinie

Sie können`AWSIoTAnalyticsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Juni 2018, 21:37 UTC
- Bearbeitete Zeit: 18. Juni 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTConfigAccess

`AWSIoTConfigAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt vollen Zugriff auf dieAWS IoT-Konfigurationsaktionen

Verwenden dieser Richtlinien

Sie können`AWSIoTConfigAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Oktober 2015, 21:52 UTC
- Bearbeitete Zeit: 27. September 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Version der Richtlinie

Version der Richtlinie:v9 (Standard)

Die Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von Berechtigungen für Berechtigungen mit den geringsten Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS mit Berechtigungen mit den geringsten Berechtigungen

AWSIoTConfigReadOnlyAccess

`AWSIoTConfigReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt nur Lesezugriff auf dieAWS IoT-Konfigurationsaktionen

Verwenden dieser -Richtlinie

Sie können`AWSIoTConfigReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Oktober 2015, 21:52 UTC
- Bearbeitete Zeit: 27. September 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTDataAccess

`AWSIoTDataAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt vollen Zugriff auf dieAWS IoT-Messaging-Aktionen

Verwenden dieser Richtlinie

Sie könnenAWSIoTDataAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Oktober 2015, 21:51 UTC
- Bearbeitete Zeit: 23. Juni 2021, 21:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDataAccess

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`ist eine AWSverwaltete Richtlinie, die: Schreibzugriff auf IoT-Dinggruppen und Lesezugriff auf IoT-Zertifikate für die Ausführung der ADD_THING_TO_THING_GROUP-Abschwächungsaktion gewährt

Verwenden dieser -Richtlinie

Sie können`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 7. August 2019, 17:55 UTC
- Bearbeitete Zeit: 7. August 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTDeviceDefenderAudit

`AWSIoTDeviceDefenderAudit`ist eine AWSverwaltete Richtlinie, die: Lesezugriff für IoT und verwandte Ressourcen bietet

Verwenden dieser -verwaltete Richtlinien

Sie können`AWSIoTDeviceDefenderAudit` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 18. Juli 2018 21:17 UTC

- Bearbeitete Zeit: 25. November 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion definiert die Berechtigungen für die -verwaltete Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten sten Berechtigungen

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`ist eine AWSverwaltete Richtlinie, die: Zugriff auf die Aktivierung der IoT-Protokollierung für die Ausführung der Schutzmaßnahme ENABLE_IOT_LOGGING bietet

Verwenden dieser -Richtlinie

Sie können`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie ist die, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit Berechtigungen mitAWS -verwaltete Richtlinien und

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`ist eine AWSverwaltete Richtlinie, die: Nachrichten den Veröffentlichungszugriff auf das SNS-Thema zur Ausführung der PUBLISH_FINDING_TO_SNS-Abschwächungsaktion gewährt

Verwenden dieser Richtlinien

Sie können`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS geringste Berechtigungen mit geringsten Berechtigungen mit geringsten Berechtigungen mit geringsten Berechtigungen

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`ist eine AWSverwaltete Richtlinie, die: Schreibzugriff auf IoT-Richtlinien für die Ausführung der Schutzmaßnahme REPLACE_DEFAULT_POLICY_VERSION gewährt

Verwenden dieser -Richtlinie

Sie können`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Richtlinie ist die -verwaltete Richtlinie, die die Berechtigungen für die -verwaltete Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien und Umstellung auf Richtlinien mit den geringsten Berechtigungen

AWSIoTDeviceDefenderUpdateCACertMitigationAction

`AWSIoTDeviceDefenderUpdateCACertMitigationAction`ist eine AWSverwaltete Richtlinie, die: Schreibzugriff auf IoT-CA-Zertifikate für die Ausführung der UPDATE_CA_CERTIFICATE-Abschwächungsmaßnahme gewährt

Verwenden dieser Richtlinie

Sie können`AWSIoTDeviceDefenderUpdateCACertMitigationAction` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 7. August 2019, 17:05 UTC
- Bearbeitete Zeit: 7. August 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine`AWS` Ressource stellt,`AWS` überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`ist eine AWSverwaltete Richtlinie, die: Schreibzugriff auf IoT-Zertifikate für die Ausführung der UPDATE_DEVICE_CERTIFICATE-Abschwächungsmaßnahme gewährt

Verwenden dieser -Richtlinie

Sie können`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 7. August 2019, 17:06 UTC
- Bearbeitete Zeit: 7. August 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTDeviceTesterForFreeRTOSFullAccess

`AWSIoTDeviceTesterForFreeRTOSFullAccess`ist einAWSverwaltete Richtliniedas: ErlaubtAWSIoT Device Tester zum Ausführen der FreeRTOS-Qualifizierungssuite, indem er den Zugriff auf Dienste wie IoT, S3 und IAM ermöglicht

Verwenden Sie diese Richtlinie

Sie können anhängen`AWSIoTDeviceTesterForFreeRTOSFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie

- Zeitpunkt der Erstellung: 12. Februar 2020, 20:33 UTC
- Bearbeitete Zeit:10. August 2023, 20:30 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Version der Richtlinie

Version der Richtlinie: v7(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSIoTDeviceTesterForGreengrassFullAccess

`AWSIoTDeviceTesterForGreengrassFullAccess`ist eine AWSverwaltete Richtlinie, die:AWS IoT Device Tester den Betrieb derAWS Greengrass-Qualifikationssuite ermöglicht, indem der Zugriff auf verwandte Dienste wie Lambda, IoT, API Gateway und IAM ermöglicht wird

Verwenden dieser -Richtlinie

Sie können`AWSIoTDeviceTesterForGreengrassFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. Februar 2020, 21:21 UTC
- Bearbeitete Zeit: 25. Juni 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTEventsFullAccess

`AWSIoTEventsFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf IoT Events bietet.

Verwenden dieser -Richtlinie

Sie können`AWSIoTEventsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 10. Januar 2019, 22:51 UTC
- Bearbeitete Zeit: 10. Januar 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTEventsReadOnlyAccess

`AWSIoTEventsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf IoT Events bietet.

Verwenden dieser -Richtlinie

Sie können`AWSIoTEventsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 10. Januar 2019, 22:50 UTC
- Bearbeitete Zeit: 23. September 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTFleetHubFederationAccess

`AWSIoTFleetHubFederationAccess`ist eine AWSverwaltete Richtlinie, die: Verbundzugriff für IoT Fleet Hub-Anwendungen

Verwenden dieser -Richtlinie

Sie können`AWSIoTFleetHubFederationAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 15. Dezember 2020, 08:08 UTC
- Bearbeitete Zeit: 4. April 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTFleetwiseServiceRolePolicy

`AWSIoTFleetwiseServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen fürAWS Ressourcen und Metadaten gewährt, die von AWSIoTFleetwise für Hilfsfunktionen verwendet oder verwaltet werden

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie

- Aufnahmezeit: 21. September 2022, 23:27 UTC
- Bearbeitete Zeit: 21. September 2022, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON policy document

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- DieAWS

AWSIoTFullAccess

`AWSIoTFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt vollen Zugriff auf dieAWS IoT-Konfiguration und die Messaging-Aktionen

Verwenden dieser -Richtlinie

Sie können`AWSIoTFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. Oktober 2015, 15:19 UTC
- Bearbeitete Zeit: 19. Mai 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTLogging

`AWSIoTLogging`ist eine AWSverwaltete Richtlinie, die: Die Erstellung von Amazon CloudWatch Log-Gruppen und Streaming-Protokollen für die Gruppen ermöglicht

Verwenden dieser -Richtlinie

Sie können`AWSIoTLogging` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 8. Oktober 2015, 15:17 UTC
- Bearbeitete Zeit: 8. Oktober 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS - verwalve

AWSIoTOTAUpdate

`AWSIoTOTAUpdate`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf das Erstellen einesAWS IoT-Jobs und die Beschreibung desAWS Codesignerjobs ermöglicht

Verwenden dieser -Richtlinie

Sie können`AWSIoTOTAUpdate` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 20. Dezember 2017, 20:36 UTC
- Bearbeitete Zeit: 20. Dezember 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIotRoboRunnerFullAccess

`AWSIotRoboRunnerFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen, die den vollen Zugriff aufAWS Iot ermöglichen RoboRunner.

Verwenden dieser Richtlinien

Sie können`AWSIotRoboRunnerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2021, 03:54 UTC
- Bearbeitete Zeit: 23. Februar 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete Richtlinie definiert die Berechtigungen für die -verwaltete Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIotRoboRunnerReadOnly

`AWSIotRoboRunnerReadOnly`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen, die nur Lesezugriff aufAWS IoT ermöglichen RoboRunner.

Verwenden dieser -Richtlinie

Sie können`AWSIotRoboRunnerReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2021, 03:43 UTC
- Bearbeitete Zeit: 16. November 2022, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIotRoboRunnerServiceRolePolicy

`AWSIotRoboRunnerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS IoT RoboRunner ermöglicht, die zugehörigenAWS Ressourcen im Namen des Kunden zu verwalten.

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 21. Februar 2023, 16:56 UTC
- Bearbeitete Zeit: 21. Februar 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  }
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTRuleActions

`AWSIoTRuleActions`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf alleAWS Dienste ermöglicht, die inAWS IoT-Regelaktionen unterstützt werden

Verwenden dieser Richtlinie

Sie können`AWSIoTRuleActions` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 8. Oktober 2015, 15:14 UTC
- Bearbeitete Zeit: 16. Januar 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTSiteWiseConsoleFullAccess

`AWSIoTSiteWiseConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die Verwaltung SiteWise vonAWS IoT mithilfe von bietetAWS Management Console. Beachten Sie, dass diese Richtlinie auch Zugriff auf das Erstellen und Auflisten von Datenspeichern gewährt, die mitAWS IoT verwendet werden SiteWise (z. B.AWS IoT Analytics), Zugriff auf das Auflisten und Anzeigen vonAWS IoT Greengrass-Ressourcen, das Auflisten und Ändern vonAWS Secrets Manager Manager-Geheimnissen, das Abrufen von Schatten vonAWS IoT-Objekten, das Auflisten von Ressourcen mit bestimmten Tags und das Erstellen und Verwenden einer dienstgebundenen Rolle fürAWS IoT SiteWise.

Verwenden dieser Richtlinien

Sie könnenAWSIoTSiteWiseConsoleFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 31. Mai 2019, 21:37 UTC
- Bearbeitete Zeit: 31. Mai 2019, 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTSiteWiseFullAccess

`AWSIoTSiteWiseFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf IoT bietet SiteWise.

Verwenden dieser -Richtlinie

Sie könnenAWSIoTSiteWiseFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. Dezember 2018, 20:53 UTC
- Bearbeitete Zeit: 4. Dezember 2018, 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSIoTSiteWiseMonitorPortalAccess

`AWSIoTSiteWiseMonitorPortalAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen für den Zugriff aufAWS SiteWise IoT-Ressourcen und Anlagendaten, die Erstellung vonAWS IoT SiteWise Monitor-Ressourcen und die Liste vonAWS SSO-Benutzern.

Verwenden dieser -Richtlinie

Sie können`AWSIoTSiteWiseMonitorPortalAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 19. Mai 2020, 20:01 UTC
- Bearbeitete Zeit: 19. Mai 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTSiteWiseMonitorServiceRolePolicy

`AWSIoTSiteWiseMonitorServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Rolle gewährtAWS SiteWise IoT-Monitorberechtigungen für den Zugriff auf IhreAWS SiteWise IoT-Ressourcen und -Anlageneigenschaften und die Erstellung vonAWS IoT Sitewise-Projekten, -Dashboards und Zugriffsrichtlinien überAWS SiteWise IoT-Portale.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 14. November 2019, 00:59 UTC
- Bearbeitete Zeit: 13. Dezember 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTSiteWiseReadOnlyAccess

`AWSIoTSiteWiseReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf IoT bietet SiteWise.

Verwenden dieser -Richtlinie

Sie könnenAWSIoTSiteWiseReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. Dezember 2018, 20:55 UTC
- Bearbeitete Zeit: 16. September 2022, 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTThingsRegistration

`AWSIoTThingsRegistration`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es Benutzern, mithilfe derAWS StartThingRegistrationTask IoT-API Dinge in großen Mengen zu registrieren

Verwenden dieser -Richtlinie

Sie können`AWSIoTThingsRegistration` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 1. Dezember 2017, 20:21 UTC
- Bearbeitete Zeit: 5. Oktober 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTTwinMakerServiceRolePolicy

`AWSIoTTwinMakerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die es AWS IoT TwinMaker ermöglicht, andere AWS Dienste aufzurufen und deren Ressourcen in Ihrem Namen zu synchronisieren.

Diese Richtlinie verwenden

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. November 2023, 18:59 UTC
- Bearbeitete Zeit: 13. November 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessDataAccess

`AWSIoTWirelessDataAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht den Zugriff auf die zugehörigen Identitätsdaten aufAWS Wireless-IoT-Geräte.

Verwenden dieser -Richtlinie

Sie können`AWSIoTWirelessDataAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 15. Dezember 2020, 15:31 UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTWirelessFullAccess

`AWSIoTWirelessFullAccess`ist eine AWSverwaltete Richtlinie, die: Der zugehörigen Identität vollen Zugriff auf alleAWS IoT-Wireless-Operationen ermöglicht.

Verwenden dieser Richtlinie

Sie können`AWSIoTWirelessFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Dezember 2020, 15:27 UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTWirelessFullPublishAccess

`AWSIoTWirelessFullPublishAccess`ist eine AWSverwaltete Richtlinie, die: IoT Wireless vollen Zugriff gewährt, um in Ihrem Namen auf der IoT Rules Engine zu veröffentlichen.

Verwenden dieser Richtlinien

Sie können`AWSIoTWirelessFullPublishAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Dezember 2020, 15:29 UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTWirelessGatewayCertManager

`AWSIoTWirelessGatewayCertManager`ist eine AWSverwaltete Richtlinie, die: Ermöglicht der zugehörigen Identität den Zugriff auf das Erstellen, Auflisten und Beschreiben von IoT-Zertifikaten

Verwenden dieser -Richtlinie

Sie können`AWSIoTWirelessGatewayCertManager` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Dezember 2020, 15:30 UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTWirelessLogging

`AWSIoTWirelessLogging`ist eine AWSverwaltete Richtlinie, die: Es der zugehörigen Identität ermöglicht, Amazon CloudWatch Logs-Gruppen zu erstellen und Protokolle an die Gruppen zu streamen.

Verwenden dieser -Richtlinie

Sie können`AWSIoTWirelessLogging` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Dezember 2020, 15:32 UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIoTWirelessReadOnlyAccess

`AWSIoTWirelessReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Der zugehörigen Identität den schreibgeschützten Zugriff aufAWS IoT-WLAN ermöglicht.

Verwenden dieser -Richtlinie

Sie können`AWSIoTWirelessReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Dezember 2020, 15:28 UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIPAMServiceRolePolicy

`AWSIPAMServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: VPC IP Address Manager den Zugriff auf VPC-Ressourcen und die Integration mit AWS Organizations in Ihrem Namen ermöglicht.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 30. November 2021, 19:08 UTC
- Bearbeitete Zeit: 8. November 2023, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIQContractServiceRolePolicy

`AWSIQContractServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: VonAWS IQ verwendet wird, um Zahlungsanfragen im Namen eines Kunden auszuführen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 22. August 2019, 19:28 UTC

- Bearbeitete Zeit: 22. August 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIQFullAccess

`AWSIQFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS IQ bietet

Verwenden dieser -Richtlinie

Sie könnenAWSIQFullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. April 2019, 23:13 UTC
- Bearbeitete Zeit: 25. September 2019, 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSIQPermissionServiceRolePolicy

`AWSIQPermissionServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS IQ ermöglicht, die vonAWS IQ-Experten übernommene Rolle zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 22. August 2019, 19:36 UTC
- Bearbeitete Zeit: 22. August 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtdokument

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

```
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf AWS Dienste und Ressourcen ermöglicht, die für benutzerdefinierte AWS KMS-Schlüsselspeicher erforderlich sind

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2018, 20:10 UTC
- Bearbeitete Zeit: 10. November 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS KMS ermöglicht, die gemeinsamen Eigenschaften von Schlüsseln mit mehreren Regionen zu synchronisieren.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 16. Juni 2021, 15:37 UTC
- Bearbeitete Zeit: 16. Juni 2021, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSKeyManagementServicePowerUser

`AWSKeyManagementServicePowerUser`ist eine AWSverwaltete Richtlinie, die: Zugriff auf denAWS Key Management Service (KMS) bietet.

Verwenden dieser -Richtlinie

Sie können`AWSKeyManagementServicePowerUser` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 7. März 2017, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLakeFormationCrossAccountManager

`AWSLakeFormationCrossAccountManager`ist eine AWSverwaltete Richtlinie, die: Kontoübergreifenden Zugriff auf Glue-Ressourcen über Lake Formation ermöglicht. Gewährt außerdem Lesezugriff auf andere erforderliche Dienste wie Organisationen und den Resource Access Manager

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSLakeFormationCrossAccountManager` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. August 2020, 20:59 UTC
- Zeit bearbeitet: 1. November 2023, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLakeFormationDataAdmin

`AWSLakeFormationDataAdmin`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff aufAWS Lake Formation und verwandte Dienste wieAWS Glue zur Verwaltung von Data Lakes gewährt

Verwenden dieser Richtlinie

Sie können`AWSLakeFormationDataAdmin` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. August 2019, 17:33 UTC
- Bearbeitete Zeit: 16. Dezember 2019, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:GetWorkflow",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
```

```
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLambda_FullAccess

`AWSLambda_FullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf denAWS Lambda-Service, dieAWS Lambda-Konsolenfunktionen und andere verwandteAWS Dienste gewährt.

Verwenden dieser -Richtlinie

Sie können`AWSLambda_FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. November 2020 21:14 UTC
- Bearbeitete Zeit: 17. November 2020, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLambda_ReadOnlyAccess

`AWSLambda_ReadOnlyAccess`ist einAWSverwaltete Richtliniedas: Gewährt schreibgeschützten Zugriff aufAWSLambda-Dienst,AWSFunktionen der Lambda-Konsole und andere verwandte FunktionenAWSdienstleistungen.

Verwendung dieser Richtlinie

Sie können anhängen`AWSLambda_ReadOnlyAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Entstehungszeit: 17. November 2020, 21:10 Uhr UTC
- Uhrzeit der Bearbeitung:27. Juli 2023, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie: v2(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eineAWSressource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSLambdaBasicExecutionRole

`AWSLambdaBasicExecutionRole`ist eine AWSverwaltete Richtlinie, die: Schreibberechtigungen für CloudWatch Logs bereitstellt.

Verwenden dieser Richtlinie

Sie können`AWSLambdaBasicExecutionRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 9. April 2015, 15:03 UTC
- Bearbeitete Zeit: 9. April 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLambdaDynamoDBExecutionRole

`AWSLambdaDynamoDBExecutionRole`ist eine AWSverwaltete Richtlinie, die: Listen- und Lesezugriff auf DynamoDB-Streams sowie Schreibrechte für CloudWatch Protokolle bereitstellt.

Verwenden dieser Richtlinien

Sie können`AWSLambdaDynamoDBExecutionRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 9. April 2015, 15:09 UTC
- Bearbeitete Zeit: 9. April 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung

AWSLambdaENIManagementAccess

`AWSLambdaENIManagementAccess`ist eine AWSverwaltete Richtlinie, die: Mindestberechtigungen für eine Lambda-Funktion zur Verwaltung von ENIs (create, describe, delete) bereitstellt, die von einer VPC-fähigen Lambda-Funktion verwendet werden.

Verwenden

Sie können`AWSLambdaENIManagementAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 6. Dezember 2016, 00:37 UTC
- Bearbeitete Zeit: 1. Oktober 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinien ist die -Richtlinie, die die Berechtigungen für die -Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalRichtlinien und Umstellung auf Berechtigungen

AWSLambdaExecute

`AWSLambdaExecute`ist eine AWSverwaltete Richtlinie, die: Put, Get-Zugriff auf S3 und vollen Zugriff auf CloudWatch Logs bietet.

Verwenden dieser -Richtlinie

Sie können`AWSLambdaExecute` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLambdaFullAccess

`AWSLambdaFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ist veraltet. Eine Anleitung finden Sie in der Dokumentation: https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based .html. Bietet vollen Zugriff auf Lambda, S3, DynamoDB, CloudWatch Metrics und Logs.

Verwenden

Sie können`AWSLambdaFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC

- Bearbeitete Zeit: 27. November 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die Standardversion definiert die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONAM-Richtlinie

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-AM-AM-AM-AM-AM-AM-AM-AM-AM-
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLambdaInvocation-DynamoDB

`AWSLambdaInvocation-DynamoDB`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf DynamoDB Streams bietet.

Verwenden dieser -Richtlinie

Sie können`AWSLambdaInvocation-DynamoDB` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -verwaltete -Richtlinie, die die Berechtigungen für die -verwaltete -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSLambdaKinesisExecutionRole

`AWSLambdaKinesisExecutionRole`ist eine AWSverwaltete Richtlinie, die: Listen- und Lesezugriff auf Kinesis-Streams sowie Schreibrechte für CloudWatch Logs bereitstellt.

Verwenden dieser -Richtlinie

Sie können`AWSLambdaKinesisExecutionRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 9. April 2015, 15:14 UTC
- Bearbeitete Zeit: 19. November 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -verwaltete -verwaltete Version, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AWSLambdaMSKExecutionRole

`AWSLambdaMSKExecutionRole`ist eine AWSverwaltete Richtlinie, die: Berechtigungen bereitstellt, die für den Zugriff auf MSK-Cluster innerhalb einer VPC, die Verwaltung von ENIs (Erstellen, Beschreiben, Löschen) in der VPC und Schreibberechtigungen für CloudWatch Logs erforderlich sind.

Verwenden dieser -Richtlinie

Sie können`AWSLambdaMSKExecutionRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 11. August 2020, 17:35 UTC
- Bearbeitete Zeit: 2. August 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLambdaReplicator

`AWSLambdaReplicator`ist eine AWSverwaltete Richtlinie, die: Lambda Replicator die erforderlichen Berechtigungen gewährt, um Funktionen regionsübergreifend zu replizieren

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 23. Mai 2017, 17:53 UTC
- Bearbeitete Zeit: 8. Dezember 2017, 00:17 UTC

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

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die die die die die die die die die die die Richtlinien für die Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSLambdaRole

`AWSLambdaRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für dieAWS Lambda-Servicerolle.

Verwenden dieser -Richtlinie

Sie können`AWSLambdaRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSLambdaSQSQueueExecutionRole

`AWSLambdaSQSQueueExecutionRole`ist eine AWSverwaltete Richtlinie, die: den Zugriff auf SQS-Warteschlangen zum Empfangen von Nachrichten, zum Löschen von Nachrichten und zum Lesen von Attributen sowie Schreibrechte für CloudWatch Protokolle bereitstellt.

Verwenden dieser -Richtlinie

Sie können`AWSLambdaSQSQueueExecutionRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. Juni 2018, 21:50 UTC
- Bearbeitete Zeit: 14. Juni 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLambdaVPCAccessExecutionRole

`AWSLambdaVPCAccessExecutionRole` ist eine -AWSverwaltete Richtlinie, die: Stellt Mindestberechtigungen für eine Lambda-Funktion bereit, die ausgeführt werden kann, während auf eine Ressource innerhalb einer VPC zugegriffen wird – Erstellen, Beschreiben, Löschen von Netzwerkschnittstellen und Schreiben von Berechtigungen in - CloudWatch Protokolle.

Verwenden dieser Richtlinie

Sie können `AWSLambdaVPCAccessExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 11. Februar 2016, 23:15 UTC
- Bearbeitungszeit: 05. Januar 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSLicenseManagerConsumptionPolicy

`AWSLicenseManagerConsumptionPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen bereitstellt, um den Zugriff auf dieAWS License Manager Manager-API-Aktionen zu ermöglichen, die für die Nutzung von Lizenzen erforderlich sind, für die der Benutzer über Berechtigungen verfügt.

Verwenden dieser -Richtlinie

Sie können`AWSLicenseManagerConsumptionPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 11. August 2021, 23:18 UTC
- Bearbeitete Zeit: 11. August 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es demAWS License Manager Linux Subscriptions Service ermöglicht, Ressourcen in Ihrem Namen zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 20. Dezember 2022, 18:54 UTC
- Bearbeitete Zeit: 20. Dezember 2022, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLicenseManagerMasterAccountRolePolicy

`AWSLicenseManagerMasterAccountRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS License Manager Service Master Account Role Policy

Verwenden dieser Richtlinie ermöglicht

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die servicegebundene Rolle an Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen an eine gebundene Rolle anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. November 2018, 19:03 UTC
- Bearbeitete Zeit: 31. Mai 2022, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-JSON-W

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen ermöglicht.

AWSLicenseManagerMemberAccountRolePolicy

`AWSLicenseManagerMemberAccountRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Rolle desAWS License Manager Manager-Dienstmitglieds

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. November 2018, 19:04 UTC

- Bearbeitete Zeit: 15. November 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:GetLicenseConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:ListAssociations"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- VerwendenAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLicenseManagerServiceRolePolicy

`AWSLicenseManagerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Standardrolle desAWS License Manager Manager-Dienstes

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. November 2018, 19:02 UTC
- Bearbeitete Zeit: 30. Juli 2021, 01:43 UTC

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

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es demAWS License Manager User Subscriptions Service ermöglicht, Ressourcen in Ihrem Namen zu verwalten.

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 30. Juli 2022, 01:17 UTC
- Bearbeitete Zeit: 21. November 2022, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-SON-SON-

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSM2ServicePolicy

`AWSM2ServicePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS M2 ermöglicht,AWS Ressourcen in Ihrem Namen zu verwalten.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 7. Juni 2022, 20:26 UTC
- Bearbeitete Zeit: 7. Juni 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standard-Version ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-----

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/M2"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSManagedServices_ContactsServiceRolePolicy

`AWSManagedServices_ContactsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Es Managed Services ermöglicht, die Werte der Tags aufAWS Ressourcen zu lesen

Verwenden

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Rollen

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 23. März 2023, 17:07 UTC
- Bearbeitete Zeit: 23. März 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

SONSONSON-Richtlinie

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Managed Services — Richtlinie zur Verwaltung der Infrastruktur für Detektivkontrollen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. Dezember 2022, 23:11 UTC
- Bearbeitete Zeit: 19. Dezember 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Richtlinie definiert die Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS

AWSManagedServices_EventsServiceRolePolicy

`AWSManagedServices_EventsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Managed Services Services-Richtlinie zur Aktivierung der AMS-Ereignisprozessorfunktion.

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die servicegebundene Rolle zugeordnet, die die die servicegebundene Rolle zugeordnet, die die die servicegebundene Rolle zugeordnet, die die Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 7. Februar 2023, 18:41 UTC
- Bearbeitete Zeit: 7. Februar 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSManagedServicesDeploymentToolkitPolicy

`AWSManagedServicesDeploymentToolkitPolicy`ist eine AWSverwaltete Richtlinie, die:AWS Es Managed Services ermöglicht, das Deployment Toolkit in Ihrem Namen zu verwalten.

Verwenden von von von dieser dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 9. Juni 2022, 18:33 UTC
- Bearbeitete Zeit: 10. Mai 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
```

```
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteLifecyclePolicy",
        "ecr:DeleteRepository",
        "ecr:DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
    }
```

```
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete

AWSMarketplaceAmiIngestion

`AWSMarketplaceAmiIngestion`ist eine AWSverwaltete Richtlinie, die: ErmöglichtAWS Marketplace das Kopieren Ihrer Amazon Machine Images (AMIs), um sie aufAWS Marketplace

Verwenden dieser -Richtlinie

Sie können`AWSMarketplaceAmiIngestion` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. September 2020, 20:55 UTC
- Bearbeitete Zeit: 25. September 2020, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceDeploymentServiceRolePolicy

`AWSMarketplaceDeploymentServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Ermöglicht AWS Marketplace die Erstellung und Verwaltung von Verkäuferbereitungsparametern für die Produkte, die Sie abonnierenAWS Marketplace.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2023, 23:34 UTC
- Bearbeitete Zeit: 15. November 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceFullAccess

`AWSMarketplaceFullAccess`ist eine AWSverwaltete Richtlinie, die: die Möglichkeit bietet,AWS Marketplace Software zu abonnieren und abzumelden, Benutzern die Verwaltung von Marketplace-Softwareinstanzen über die Marketplace-Seite „Ihre Software“ ermöglicht und administrativen Zugriff auf EC2 bietet.

Verwenden dieser -Richtlinie

Sie können`AWSMarketplaceFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Februar 2015, 17:21 UTC
- Bearbeitete Zeit: 4. März 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceGetEntitlements

`AWSMarketplaceGetEntitlements`ist eine AWSverwaltete Richtlinie, die: Lesezugriff aufAWS Marketplace Berechtigungen gewährt

Verwenden dieser -Richtlinie

Sie können`AWSMarketplaceGetEntitlements` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. März 2017, 19:37 UTC
- Bearbeitete Zeit: 27. März 2017, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceImageBuildFullAccess

`AWSMarketplaceImageBuildFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf dieAWS Marketplace Private Image Build-Funktion bietet. Neben der Erstellung privater Images bietet es auch Berechtigungen zum Hinzufügen von Tags zu Bildern sowie zum Starten und Beenden von ec2-Instances.

Verwenden dieser Richtlinie

Sie können`AWSMarketplaceImageBuildFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 31. Juli 2018, 23:29 UTC
- Bearbeitete Zeit: 4. März 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für

den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceLicenseManagementServiceRolePolicy

`AWSMarketplaceLicenseManagementServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und Ressourcen ermöglicht, dieAWS Marketplace für die Lizenzverwaltung verwendet oder verwaltet werden.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 3. Dezember 2020, 08:33 UTC
- Bearbeitete Zeit: 3. Dezember 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Durchführung der Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-----

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListReceivedGrants",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant",
        "license-manager:AcceptGrant"
      ],
```

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions`ist eine AWSverwaltete Richtlinie, die: Die Möglichkeit bietet,AWS Marketplace Software zu abonnieren und abzumelden

Verwenden dieser -Richtlinie

Sie können`AWSMarketplaceManageSubscriptions` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 19. Januar 2023, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceMeteringFullAccess

`AWSMarketplaceMeteringFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS Marketplace Metering bietet.

Verwenden dieser -Richtlinie

Sie können`AWSMarketplaceMeteringFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. März 2016, 22:39 UTC
- Bearbeitete Zeit: 17. März 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceMeteringRegisterUsage

`AWSMarketplaceMeteringRegisterUsage`ist eine AWSverwaltete Richtlinie, die: Berechtigungen zur Registrierung einer Ressource und zur Nachverfolgung der Nutzung über denAWS Marketplace Metering Service bereitstellt.

Verwenden dieser -Richtlinie

Sie können`AWSMarketplaceMeteringRegisterUsage` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 21. November 2019, 01:17 UTC
- Bearbeitete Zeit: 21. November 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceProcurementSystemAdminFullAccess

`AWSMarketplaceProcurementSystemAdminFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf alle administrativen Aktionen für eineAWS Marketplace eProcurement-Integration bietet.

Verwenden dieser Richtlinie

Sie können`AWSMarketplaceProcurementSystemAdminFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 25. Juni 2019, 13:07 UTC
- Bearbeitete Zeit: 25. Juni 2019, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplacePurchaseOrdersServiceRolePolicy

`AWSMarketplacePurchaseOrdersServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS Marketplace Dienste zur Bestellverwaltung ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 27. Oktober 2021, 15:12 UTC
- Bearbeitete Zeit: 27. Oktober 2021, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version zugeordnet, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONSONSONSONSONSON

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

```
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceRead-only

`AWSMarketplaceRead-only`ist eine AWSverwaltete Richtlinie, die: Die Möglichkeit bietet,AWS Marketplace Abonnements zu überprüfen

Verwenden dieser -Richtlinie

Sie können`AWSMarketplaceRead-only` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 19. Januar 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceResaleAuthorizationServiceRolePolicy

`AWSMarketplaceResaleAuthorizationServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Aktiviert den Zugriff auf AWS-Services und Ressourcen, die von AWS Marketplace für die Wiederverkaufsautorisierung verwendet oder verwaltet werden.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 05. März 2024, 18:47 UTC
- Bearbeitungszeit: 05. März 2024, 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMarketplaceSellerFullAccess

`AWSMarketplaceSellerFullAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf alle Verkäuferoperationen auf dem AWS Marketplace und anderen - AWS Services wie AMI-Management.

Verwenden dieser Richtlinie

Sie können `AWSMarketplaceSellerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 02. Juli 2019, 20:40 UTC

- Bearbeitungszeit: 15. März 2024, 16:09 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Richtlinienversion

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerProductsFullAccess

`AWSMarketplaceSellerProductsFullAccess`ist einAWSverwaltete Richtliniedas: Bietet Verkäufern vollen Zugriff aufAWS MarketplaceSeite „Management-Produkte“ und andereAWSDienste wie AMI-Management.

Verwendung dieser Richtlinie

Sie können anhängen`AWSMarketplaceSellerProductsFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 02. Juli 2019, 21:06 Uhr UTC
- Uhrzeit der Bearbeitung:18. Juli 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Version der Richtlinie

Version der Richtlinie: v7(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerProductsReadOnly

`AWSMarketplaceSellerProductsReadOnly`ist eine AWSverwaltete Richtlinie, die: Verkäufern Lesezugriff auf die Seite „AWS MarketplaceVerwaltungsprodukte“ gewähren.

Verwenden dieser -Richtlinie

Sie können`AWSMarketplaceSellerProductsReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. Juli 2019, 21:40 UTC
- Bearbeitete Zeit: 19. November 2022, 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMediaConnectServicePolicy

`AWSMediaConnectServicePolicy`ist eine AWSverwaltete Richtlinie, die: Die Standardrichtlinie, die den Zugriff aufAWS-Services und Ressourcen ermöglicht, von denen sie verwendet oder verwaltet werden MediaConnect.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 3. April 2023, 22:11 UTC
- Bearbeitete Zeit: 3. April 2023, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standard-Version der Richtlinie definiert die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienlinienlinien

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMediaTailorServiceRolePolicy

`AWSMediaTailorServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS Ressourcen ermöglicht, die verwendet oder verwaltet werden von MediaTailor

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. September 2021, 22:27 UTC
- Bearbeitete Zeit: 17. September 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die -Richtlinie definiert, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-JSON-Richtlinien

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

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMigrationHubDiscoveryAccess

`AWSMigrationHubDiscoveryAccess`ist eine AWSverwaltete Police, die: Die Richtlinie es AWSMigrationHubService ermöglicht, AWSApplicationDiscoveryService im Namen des Kunden anzurufen.

Verwenden dieser -Richtlinie

Sie können`AWSMigrationHubDiscoveryAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. August 2017, 13:30 UTC
- Bearbeitete Zeit: 06. August 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMigrationHubDMSAccess

`AWSMigrationHubDMSAccess`ist eine AWSverwaltete Richtlinie, die: Richtlinie, nach der der Database Migration Service die Rolle im Kundenkonto übernimmt und Migration Hub anruft

Verwenden dieser Richtlinien

Sie können`AWSMigrationHubDMSAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. August 2017, 14:00 UTC
- Bearbeitete Zeit: 7. Oktober 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMigrationHubFullAccess

`AWSMigrationHubFullAccess`ist eine AWSverwaltete Richtlinie, die: Verwaltete Richtlinie, um dem Kunden Zugriff auf den Migration Hub Service zu gewähren

Verwenden dieser Richtlinie

Sie können`AWSMigrationHubFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. August 2017, 14:02 UTC
- Bearbeitete Zeit: 19. Juni 2019, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMigrationHubOrchestratorConsoleFullAccess

`AWSMigrationHubOrchestratorConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: eingeschränkten Zugriff auf AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service und AWS Secrets Manager bietet. Diese Richtlinie gewährt auch vollen Zugriff auf den AWS Migration Hub Orchestrator-Dienst.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSMigrationHubOrchestratorConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. April 2022, 02:26 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorInstanceRolePolicy

`AWSMigrationHubOrchestratorInstanceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie für migrierte SAP- und MGN-Instanzen angehängt werden muss, damit unser Service Instanzen orchestriert, indem Skripts von S3 heruntergeladen und geheime Werte innerhalb der EC2-Instance abgerufen werden.

Verwenden dieser -Richtlinie

Sie können`AWSMigrationHubOrchestratorInstanceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. April 2022, 02:43 UTC
- Bearbeitete Zeit: 20. April 2022, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMigrationHubOrchestratorPlugin

`AWSMigrationHubOrchestratorPlugin`ist eine AWSverwaltete Richtlinie, die: Eingeschränkten Zugriff auf Amazon Simple Storage Service,AWS Secrets Manager und Plugin-bezogene Aktionen fürAWS Migration Hub Orchestrator bietet.

Verwenden dieser -Richtlinie

Sie können`AWSMigrationHubOrchestratorPlugin` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. April 2022, 02:25 UTC
- Bearbeitete Zeit: 20. April 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von -IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMigrationHubOrchestratorServiceRolePolicy

`AWSMigrationHubOrchestratorServiceRolePolicy` ist eine -AWS verwaltete Richtlinie, die: Stellt Berechtigungen bereit, die für Migration Hub Orchestrator erforderlich sind, um Ihre On-Premises-Workloads zu migrieren und zu modernisieren

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 20. April 2022, 02:24 UTC
- Bearbeitungszeit: 04. März 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
```

```
  "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-*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`ist einAWSverwaltete Richtliniedas: Gewährt vollen Zugriff aufAWSMigration Hub, Refactor Spaces und andereAWSverwandte Dienstleistungen außerAWSTransit Gateway und EC2-Sicherheitsgruppen sind nicht erforderlich, wenn Umgebungen ohne Netzwerkbrücke verwendet werden. Diese Richtlinie schließt auch Berechtigungen aus, die erforderlich sind fürAWSLambda undAWSResource Access Manager, da sie anhand von Tags eingeschränkt werden können.

Verwendung dieser Richtlinie

Sie können anhängen`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie

- Zeit der Erstellung: 03. April 2023, 20:09 Uhr UTC
- Uhrzeit der Bearbeitung:20. Juli 2023, 15:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Version der Richtlinie

Version der Richtlinie: v2(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
```

```
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`ist einAWSverwaltete Richtliniedas: Verwendung in der IAM-Servicerolle, die an das SSM-Automatisierungsdokument übergeben wurde AWSRefactorSpaces-CreateResources um die für die Ausführung der Automatisierung erforderlichen Berechtigungen zu erteilen. Die Richtlinie gewährt Lese-/Schreibzugriff auf EC2-Tags, um den Automatisierungsfortschritt zu verfolgen. Wenn die Netzwerkbrücke der Refactor Spaces-Umgebung aktiviert ist, fügt die Automatisierung der EC2-Instance auch die Sicherheitsgruppe der Umgebung hinzu, um Datenverkehr von anderen Refactor Spaces-Diensten in der Umgebung zuzulassen. Die Richtlinie gewährt auch Zugriff auf die SSM-Parameter für Aktionen nach dem Start des Application Migration Service.

Verwenden Sie diese Richtlinie

Sie können anhängen`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Zeit der Erstellung: 10. August 2023, 15:08 Uhr UTC
- Bearbeitete Zeit:10. August 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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-
*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpacesFullAccess

`AWSMigrationHubRefactorSpacesFullAccess`ist einAWSverwaltete Richtliniedas: Gewährt vollen Zugriff aufAWS MigrationHubRäume umgestalten,AWS MigrationHubFunktionen der Refactor Spaces-Konsole und andere verwandte FunktionenAWSDienste außer den erforderlichen Genehmigungen fürAWSLambda undAWSResource Access Manager, da sie anhand von Tags eingeschränkt werden können.

Verwendung dieser Richtlinie

Sie können anhängen`AWSMigrationHubRefactorSpacesFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 29. November 2021, 07:12 Uhr UTC
- Uhrzeit der Bearbeitung:19. Juli 2023, 19:07 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Version der Richtlinie

Version der Richtlinie: v5(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTransitGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
```

```
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpacesServiceRolePolicy

`AWSMigrationHubRefactorSpacesServiceRolePolicy`ist einAWSverwaltete Richtliniedas: Bietet Zugriff aufAWSRessourcen, die verwaltet oder genutzt werden vonAWSMigration Hub Refactor Spaces.

Verwendung dieser Richtlinie

Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen auszuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstbezogene Rollen
- Zeit der Erstellung: 29. November 2021, 06:50 Uhr UTC
- Uhrzeit der Bearbeitung:20. Juli 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie: v3(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSMigrationHubSMSAccess

`AWSMigrationHubSMSAccess`ist eine AWSverwaltete Richtlinie, die: Richtlinie, nach der der Server Migration Service die Rolle im Kundenkonto übernimmt und Migration Hub aufruft

Verwenden dieser Richtlinie

Sie können`AWSMigrationHubSMSAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. August 2017, 13:57 UTC
- Bearbeitete Zeit: 7. Oktober 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSMigrationHubStrategyCollector

`AWSMigrationHubStrategyCollector` ist eine -AWSverwaltete Richtlinie, die: Gewährt Berechtigungen, um die Kommunikation mit dem AWS Migration Hub Strategy Recommendations-Service, Lese-/Schreibzugriff auf S3-Buckets im Zusammenhang mit dem Service, Amazon API Gateway-Zugriff zum Hochladen von Protokollen und Metriken in AWS, AWS Secrets Manager-Zugriff zum Abrufen von Anmeldeinformationen und allen zugehörigen -Services zu ermöglichen.

Verwenden dieser Richtlinie

Sie können `AWSMigrationHubStrategyCollector` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 19. Oktober 2021, 20:15 UTC
- Bearbeitungszeit: 05. Februar 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Richtlinienversion

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowMetricsAndLogs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:PutMetricData",
        "application-transformation:PutLogData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MHSRAllowExecuteAPI",
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Sid" : "MHSRAllowCollectorAPI",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:RegisterCollector",
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration"
      ],
      "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
    },
    {
      "Sid" : "MHSRAllowSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSMigrationHubStrategyConsoleFullAccess

`AWSMigrationHubStrategyConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den DienstAWS Migration Hub Strategy Recommendations und Zugriff auf verwandteAWS Dienste über denAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AWSMigrationHubStrategyConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 19. Oktober 2021, 20:13 UTC
- Bearbeitete Zeit: 9. November 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwaltete -verwaltete Version ist die -verwaltete Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-AM-AM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMigrationHubStrategyServiceRolePolicy

`AWSMigrationHubStrategyServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS Ressourcen ermöglicht, die vomAWS Migration Hub Strategy Recommendations Service verwendet oder verwaltet werden.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. Oktober 2021, 20:02 UTC
- Bearbeitete Zeit: 19. Oktober 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMobileHub_FullAccess

`AWSMobileHub_FullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie kann an jeden Benutzer, jede Rolle oder Gruppe angehängt werden, um Benutzern die Erlaubnis zu gewähren, Projekte (und die zugehörigenAWS Ressourcen) inAWS Mobile Hub zu erstellen, zu löschen und zu ändern. Dazu gehören auch die Berechtigungen zum Generieren und Herunterladen von Beispielquellcode für mobile Apps für jedes Mobile Hub Hub-Projekt.

Verwenden dieser Richtlinien

Sie könnenAWSMobileHub_FullAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. Januar 2016, 19:56 UTC
- Bearbeitete Zeit: 19. Dezember 2019, 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

Version der Richtlinie

Version der Richtlinie:v14 (Standard)

Die Standardversion definiert die Berechtigungen definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AWSMobileHub_ReadOnly

`AWSMobileHub_ReadOnly`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie kann an jeden Benutzer, jede Rolle oder Gruppe angehängt werden, um Benutzern die Erlaubnis zu gewähren, Projekte inAWS Mobile Hub aufzulisten und anzusehen. Dazu gehören auch die Berechtigungen zum Generieren und Herunterladen von Beispielquellcode für mobile Apps für jedes Mobile Hub Hub-Projekt. Es erlaubt dem Benutzer nicht, eine Konfiguration für ein Mobile Hub Hub-Projekt zu ändern.

Verwenden dieser -Richtlinie

Sie können`AWSMobileHub_ReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 5. Januar 2016, 19:55 UTC
- Bearbeitete Zeit: 23. Juli 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Version der Richtlinie

Version der Richtlinie:v10 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSMSKReplicatorExecutionRole

`AWSMSKReplicatorExecutionRole`ist eine AWSverwaltete Richtlinie, die: Amazon MSK Replicator die Erlaubnis erteilt, Daten zwischen MSK-Clustern zu replizieren.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMSKReplicatorExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Dezember 2023, 00:07 Uhr UTC
- Bearbeitete Zeit: 6. Dezember 2023, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "TopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:AlterCluster"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:topic/*/*"
      ]
    },
```

```
    {
      "Sid" : "GroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:group/*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkFirewallServiceRolePolicy

`AWSNetworkFirewallServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Ermöglicht AWSNetworkFirewall die Erstellung und Verwaltung der erforderlichen Ressourcen für Ihre Firewalls.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. November 2020, 17:17 UTC
- Bearbeitete Zeit: 30. März 2023, 17:19 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSNetworkManagerCloudWANServiceRolePolicy

`AWSNetworkManagerCloudWANServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: NetworkManager den Zugriff auf Ressourcen ermöglicht, die Ihrem Kernnetzwerk zugeordnet sind

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. Juli 2022, 12:17 UTC
- Bearbeitete Zeit: 12. Juli 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Durchführung von Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
```

```
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSNetworkManagerFullAccess

`AWSNetworkManagerFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon NetworkManager über die bietetAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AWSNetworkManagerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 17:37 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSNetworkManagerReadOnlyAccess

`AWSNetworkManagerReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht Lesezugriff auf Amazon NetworkManager über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie könnenAWSNetworkManagerReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Dezember 2019, 17:35 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSNetworkManagerServiceRolePolicy

`AWSNetworkManagerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: NetworkManager den Zugriff auf Ressourcen ermöglicht, die mit Ihren globalen Netzwerken verknüpft sind

Verwenden von von von von von

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 3. Dezember 2019, 14:03 UTC
- Bearbeitete Zeit: 27. Juli 2022, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die Standardversion der Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS

AWSOpsWorks_FullAccess

`AWSOpsWorks_FullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf bietetAWS OpsWorks.

Verwenden dieser Richtlinie

Sie können`AWSOpsWorks_FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. Januar 2021, 16:29 UTC
- Bearbeitete Zeit: 22. Januar 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit denAWS geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOpsWorksCloudWatchLogs

`AWSOpsWorksCloudWatchLogs`ist eine AWSverwaltete Richtlinie, die: OpsWorks Instanzen mit aktivierter CWLogs-Integration den Versand von Protokollen und das Erstellen erforderlicher Protokollgruppen ermöglicht

Verwenden dieser -Richtlinie

Sie können`AWSOpsWorksCloudWatchLogs` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. März 2017, 17:47 UTC
- Bearbeitete Zeit: 30. März 2017, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOpsWorksCMInstanceProfileRole

`AWSOpsWorksCMInstanceProfileRole`ist eine AWSverwaltete Richtlinie, die: S3-Zugriff für Instances bietet, die von OpsWorks CM gestartet wurden.

Verwenden dieser -Richtlinie

Sie können`AWSOpsWorksCMInstanceProfileRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. November 2016, 09:48 UTC
- Bearbeitete Zeit: 23. April 2021, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOpsWorksCMServiceRole

`AWSOpsWorksCMServiceRole`ist eine AWSverwaltete Richtlinie, die: Service Role Policy, die für die Erstellung von OpsWorks CM-Servern verwendet werden soll.

Verwenden dieser -Richtlinie

Sie können`AWSOpsWorksCMServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 24. November 2016, 09:49 UTC
- Bearbeitete Zeit: 23. April 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

Version der Richtlinie

Version der Richtlinie:v14 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOpsWorksInstanceRegistration

`AWSOpsWorksInstanceRegistration`ist eine AWSverwaltete Richtlinie, die: Ermöglicht den Zugriff auf eine Amazon EC2 EC2-Instance, um sich bei einemAWS OpsWorks Stack zu registrieren.

Verwenden dieser -Richtlinie

Sie können`AWSOpsWorksInstanceRegistration` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. Juni 2016, 14:23 UTC
- Bearbeitete Zeit: 3. Juni 2016, 14:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für

den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:RegisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOpsWorksRegisterCLI_EC2

`AWSOpsWorksRegisterCLI_EC2`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung der Registrierung von EC2-Instances über die OpsWorks CLI

Verwenden dieser -Richtlinie

Sie können`AWSOpsWorksRegisterCLI_EC2` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Juni 2019, 15:56 UTC
- Bearbeitete Zeit: 18. Juni 2019, 15:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von -IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOpsWorksRegisterCLI_OnPremises

`AWSOpsWorksRegisterCLI_OnPremises`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung der Registrierung von On-Premises-Instanzen über die OpsWorks CLI

Verwenden dieser -diese -verwaltete

Sie können`AWSOpsWorksRegisterCLI_OnPremises` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 18. Juni 2019, 15:33 UTC
- Bearbeitete Zeit: 18. Juni 2019, 15:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete -verwaltete -verwaltete Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOrganizationsFullAccess

`AWSOrganizationsFullAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf AWS Organizations.

Verwenden dieser Richtlinie

Sie können `AWSOrganizationsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. November 2018, 20:31 UTC
- Bearbeitungszeit: 06. Februar 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Richtlinienversion

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSOrganizationsReadOnlyAccess

`AWSOrganizationsReadOnlyAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf AWS Organizations.

Verwenden dieser Richtlinie

Sie können `AWSOrganizationsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. November 2018, 20:32 UTC
- Bearbeitungszeit: 06. Februar 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOrganizationsServiceTrustPolicy

`AWSOrganizationsServiceTrustPolicy`ist eine AWSverwaltete Richtlinie, die: Eine Richtlinie, die esAWS Organizations ermöglicht, Vertrauen mit anderen zugelassenenAWS-Services Personen zu teilen, um die Kundenkonfiguration zu vereinfachen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 10. Oktober 2017, 23:04 UTC
- Bearbeitete Zeit: 1. November 2017, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOutpostsAuthorizeServerPolicy

`AWSOutpostsAuthorizeServerPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen, mit denen Sie einen Outpost-Server in Ihrem lokalen Netzwerk installieren können.

Verwenden dieser -Richtlinie

Sie könnenAWSOutpostsAuthorizeServerPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. Januar 2023, 19:23 UTC
- Bearbeitete Zeit: 4. Januar 2023, 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSOutpostsServiceRolePolicy

`AWSOutpostsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Service Linked Role-Richtlinie, um den Zugriff aufAWS Ressourcen zu ermöglichen, die vonAWS Outposts verwaltet werden

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen angehängt.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 9. November 2020, 22:55 UTC
- Bearbeitete Zeit: 9. November 2020, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Richtlinie ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

Richtlinien

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AWSPanoramaApplianceRolePolicy

`AWSPanoramaApplianceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS IoT-Software auf einerAWS Panorama-Appliance ermöglicht, Protokolle auf Amazon hochzuladen CloudWatch.

Verwenden dieser -Richtlinie

Sie können`AWSPanoramaApplianceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 1. Dezember 2020, 13:13 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPanoramaApplianceServiceRolePolicy

`AWSPanoramaApplianceServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es einerAWS Panorama-Appliance ermöglicht CloudWatch, Protokolle auf Amazon hochzuladen und Objekte von Amazon S3 S3-Access Points abzurufen, die für die Verwendung mitAWS Panorama erstellt wurden.

Verwenden dieser -Richtlinie

Sie können`AWSPanoramaApplianceServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 20. Oktober 2021, 12:14 UTC
- Bearbeitete Zeit: 17. Januar 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPanoramaFullAccess

`AWSPanoramaFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Panorama bietet

Verwenden dieser -Richtlinie

Sie können`AWSPanoramaFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2020, 13:12 UTC
- Bearbeitete Zeit: 12. Januar 2022, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPanoramaGreengrassGroupRolePolicy

`AWSPanoramaGreengrassGroupRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es einerAWS Lambda-Funktion auf einerAWS Panorama-Appliance ermöglicht, Ressourcen in Panorama zu verwalten, Protokolle und Metriken auf Amazon hochzuladen und Objekte in Buckets zu verwalten CloudWatch, die für die Verwendung mit Panorama erstellt wurden.

Verwenden dieser -Richtlinie

Sie könnenAWSPanoramaGreengrassGroupRolePolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 1. Dezember 2020, 13:10 UTC
- Bearbeitete Zeit: 6. Januar 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPanoramaSageMakerRolePolicy

`AWSPanoramaSageMakerRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon SageMaker die Verwaltung von Objekten in Buckets ermöglicht, die für die Verwendung mitAWS Panorama erstellt wurden.

Verwenden dieser -Richtlinie

Sie können`AWSPanoramaSageMakerRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 1. Dezember 2020, 13:13 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPanoramaServiceLinkedRolePolicy

`AWSPanoramaServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Panorama die Verwaltung von Ressourcen inAWS IoT,AWS Secrets Manager undAWS Panorama ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 20. Oktober 2021, 12:12 UTC
- Bearbeitete Zeit: 20. Oktober 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standards-Richtlinie ist die -Standards-JSON-Richt Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON----Richt

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSPanoramaServiceRolePolicy

`AWSPanoramaServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Panorama ermöglicht, Ressourcen in Amazon S3,AWSAWS IoT GreenGrass,AWS Lambda SageMaker,

Amazon und Amazon CloudWatch Logs zu verwalten und Servicerollen anAWS IoT GreenGrass,AWS IoT und Amazon zu übergeben SageMaker.

Verwenden dieser -Richtlinie

Sie könnenAWSPanoramaServiceRolePolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 1. Dezember 2020, 13:14 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 13:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete Version ist die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPriceListServiceFullAccess

`AWSPriceListServiceFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf denAWS Price List Service bietet.

Verwenden dieser -Richtlinie

Sie können`AWSPriceListServiceFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. November 2017 00:36 UTC
- Bearbeitete Zeit: 22. November 2017, 00:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "pricing:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPrivateCAAuditor

`AWSPrivateCAAuditor`ist eine AWSverwaltete Richtlinie, die: Auditoren Zugriff auf dieAWS Private Certificate Authority gewährt

Verwenden dieser -Richtlinie

Sie können`AWSPrivateCAAuditor` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Februar 2023, 18:33 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPrivateCAFullAccess

`AWSPrivateCAFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS Private Certificate Authority bietet

Verwenden dieser Richtlinie

Sie können`AWSPrivateCAFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Februar 2023, 18:20 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:20 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardrichtlinie definiert die Berechtigungen für die -Standardrichtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPrivateCAPrivilegedUser

`AWSPrivateCAPrivilegedUser`ist eine AWSverwaltete Richtlinie, die: Privilegierten Zertifikatsbenutzern Zugriff aufAWS Private Certificate Authority gewährt

Verwenden dieser Richtlinien

Sie könnenAWSPrivateCAPrivilegedUser an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Februar 2023, 18:26 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Funktion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPrivateCAReadOnly

`AWSPrivateCAReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS Private Certificate Authority gewährt

Verwenden dieser -Richtlinie

Sie können`AWSPrivateCAReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Februar 2023, 18:30 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPrivateCAUser

`AWSPrivateCAUser`ist eine AWSverwaltete Richtlinie, die: Zertifikatsbenutzern Zugriff aufAWS Private Certificate Authority gewährt

Verwenden dieser -Richtlinie

Sie können`AWSPrivateCAUser` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Februar 2023, 18:16 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPrivateMarketplaceAdminFullAccess

`AWSPrivateMarketplaceAdminFullAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf alle administrativen Aktionen für einen AWS Private Marketplace.

Verwenden dieser Richtlinie

Sie können `AWSPrivateMarketplaceAdminFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 16:32 UTC
- Bearbeitungszeit: 14. Februar 2024, 22:05 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Richtlinienversion

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSPrivateMarketplaceRequests

`AWSPrivateMarketplaceRequests`ist eine AWSverwaltete Richtlinie, die: Zugriff auf das Erstellen von Anfragen auf einemAWS privaten Marketplace bietet.

Verwenden dieser -Richtlinie

Sie könnenAWSPrivateMarketplaceRequests an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. Oktober 2019, 21:44 UTC
- Bearbeitete Zeit: 28. Oktober 2019, 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Version. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von -IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSPrivateNetworksServiceRolePolicy

`AWSPrivateNetworksServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Private Networks Service die Verwaltung von Ressourcen im Namen des Kunden ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 16. Dezember 2021, 23:17 UTC
- Bearbeitete Zeit: 16. Dezember 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die die die die die die Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSProtonCodeBuildProvisioningBasicAccess

`AWSProtonCodeBuildProvisioningBasicAccess`ist eine AWSverwaltete Richtlinie, die: CodeBuild Berechtigungen benötigen, um einen Build fürAWS Proton CodeBuild Provisioning auszuführen.

Verwenden dieser Richtlinie

Sie können`AWSProtonCodeBuildProvisioningBasicAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. November 2022, 21:04 UTC
- Bearbeitete Zeit: 9. November 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSProtonCodeBuildProvisioningServiceRolePolicy

`AWSProtonCodeBuildProvisioningServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS Proton ermöglicht, die Bereitstellung von Proton-RessourcenCodeBuild und andereAWS Dienste in Ihrem Namen zu verwalten.

Verwenden von Verwenden von Verwenden von Verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 9. November 2022, 21:32 UTC
- Bearbeitete Zeit: 17. Mai 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

Dokument, die JSON-Richtlinie

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSProtonDeveloperAccess

`AWSProtonDeveloperAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf dieAWS Proton-APIs und die Management Console bietet, jedoch keine Verwaltung von Proton-Vorlagen oder -Umgebungen ermöglicht.

Verwenden

Sie können`AWSProtonDeveloperAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. Februar 2021, 19:02 UTC
- Bearbeitete Zeit: 18. November 2022, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -verwaltete -Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSProtonFullAccess

`AWSProtonFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf dieAWS Proton-APIs und die Management Console bietet. Zusätzlich zu diesen Berechtigungen ist auch Zugriff auf Amazon S3 erforderlich, um Vorlagenpakete aus Ihren S3-Buckets zu registrieren, sowie Zugriff auf Amazon IAM, um die Servicerollen für Proton zu erstellen und zu verwalten.

Verwenden dieser Richtlinie

Sie können`AWSProtonFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. Februar 2021, 19:07 UTC
- Bearbeitete Zeit: 20. Juni 2022, 12:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSProtonReadOnlyAccess

`AWSProtonReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf dieAWS Proton-APIs und die Management Console bietet.

Verwenden dieser -Richtlinie

Sie können`AWSProtonReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. Februar 2021, 19:09 UTC
- Bearbeitete Zeit: 18. November 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die Berechtigungen für die -die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Berechtigungen mit den geringsten Berechtigungen

AWSProtonServiceGitSyncServiceRolePolicy

`AWSProtonServiceGitSyncServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die esAWS Proton ermöglicht, Ihre Dienst-, Umgebungs- und Komponentendefinitionen aus Ihrem Git-Repository mitAWS Proton zu synchronisieren.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die der Service die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 4. April 2023, 15:55 UTC
- Bearbeitete Zeit: 4. April 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie definiert die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSProtonSyncServiceRolePolicy

`AWSProtonSyncServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die esAWS Proton ermöglicht, Ihre Git-Repository-Inhalte mit Proton zu synchronisieren oder Proton-Inhalte mit Ihren Git-Repositorys zu synchronisieren.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 23. November 2021, 21:14 UTC
- Bearbeitete Zeit: 23. November 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die -Richtlinie, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
```

```
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AWSPurchaseOrdersServiceRolePolicy

`AWSPurchaseOrdersServiceRolePolicy`ist einAWSverwaltete Richtliniedas: Erteilt Berechtigungen zum Anzeigen und Ändern von Bestellungen in der Abrechnungskonsole

Verwendung dieser Richtlinie

Sie können anhängen`AWSPurchaseOrdersServiceRolePolicy`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 06. Mai 2020, 18:15 Uhr UTC
- Uhrzeit der Bearbeitung:17. Juli 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie: v5(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
```

```
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSQuicksightAthenaAccess

`AWSQuicksightAthenaAccess`ist eine AWSverwaltete Richtlinie, die: Quicksight-Zugriff auf Athena-API und S3-Buckets, die für Athena-Abfrageergebnisse verwendet werden

Verwenden dieser Richtlinie

Sie können`AWSQuicksightAthenaAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 9. Dezember 2016, 02:31 UTC
- Bearbeitete Zeit: 7. Juli 2021, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Version der Richtlinie

Version der Richtlinie:v10 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSQuickSightDescribeRDS

`AWSQuickSightDescribeRDS`Sist eine AWSverwaltete Richtlinie, die: QuickSight die Beschreibung der RDS-Ressourcen ermöglicht

Verwenden dieser -Richtlinie

Sie können`AWSQuickSightDescribeRDS` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 10. November 2015, 23:24 UTC
- Bearbeitete Zeit: 10. November 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSQuickSightDescribeRedshift

`AWSQuickSightDescribeRedshift`ist eine AWSverwaltete Richtlinie, die: QuickSight die Beschreibung von Redshift-Ressourcen ermöglicht

Verwenden dieser -Richtlinie

Sie können`AWSQuickSightDescribeRedshift` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 10. November 2015, 23:25 UTC
- Bearbeitete Zeit: 10. November 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSQuickSightElasticsearchPolicy

`AWSQuickSightElasticsearchPolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Amazon Elasticsearch-Ressourcen von Amazon bietet QuickSight

Verwenden dieser -Richtlinie

Sie können`AWSQuickSightElasticsearchPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 9. September 2020, 17:27 UTC
- Bearbeitete Zeit: 7. September 2021, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Standardrichtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSQuickSightIoTAnalyticsAccess

`AWSQuickSightIoTAnalyticsAccess`ist eine AWSverwaltete Richtlinie, die: QuickSight Lesezugriff auf IoT Analytics Analytics-Datensätze gewährt

Verwenden dieser -Richtlinie

Sie können`AWSQuickSightIoTAnalyticsAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2017, 17:00 UTC
- Bearbeitete Zeit: 29. November 2017, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -verwaltete Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iotanalytics:ListDatasets",
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSQuickSightListIAM

`AWSQuickSightListIAM`ist eine AWSverwaltete Richtlinie, die: Erlaubt QuickSight das Auflisten von IAM-Entitäten

Verwenden dieser Richtlinien

Sie könnenAWSQuickSightListIAM an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 10. November 2015, 23:25 UTC
- Bearbeitete Zeit: 10. November 2015, 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Version ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSQuicksightOpenSearchPolicy

`AWSQuicksightOpenSearchPolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf OpenSearch Amazon-Ressourcen von Amazon bietet QuickSight

Verwenden dieser -Richtlinie

Sie können`AWSQuicksightOpenSearchPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 7. September 2021, 23:26 UTC
- Bearbeitete Zeit: 7. September 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSQuickSightSageMakerPolicy

`AWSQuickSightSageMakerPolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf SageMaker Amazon-Ressourcen von Amazon ermöglicht QuickSight

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightSageMakerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. Januar 2020, 17:18 Uhr UTC
- Bearbeitete Zeit: 30. Oktober 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightTimestreamPolicy

`AWSQuickSightTimestreamPolicy`ist eine AWSverwaltete Richtlinie, die:AWS QuickSight Zugriff aufAWS Timestream-APIs. Kunden können diese Richtlinie an dieAWS QuickSight Rolle anhängen, um das Abrufen von Daten und Metadaten zu ermöglichen.

Verwenden dieser -Richtlinie

Sie können`AWSQuickSightTimestreamPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 30. September 2020, 21:47 UTC
- Bearbeitete Zeit: 30. September 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSReachabilityAnalyzerServiceRolePolicy

`AWSReachabilityAnalyzerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: VPC Reachability Analyzer den Zugriff auf AWS Ressourcen und die Integration in AWS Organisationen in Ihrem Namen ermöglicht.

Verwendung dieser Richtlinie

Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen auszuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstverknüpfte Rollen
- Aufnahmezeit: 23. November 2022, 17:12 UTC
- Bearbeitete Zeit: 23. Juni 2023, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AWSRefactoringToolkitFullAccess

`AWSRefactoringToolkitFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt die Erlaubnis zur Nutzung von AWS Diensten mit der AWS Toolkit for .NET Refactoring-Erweiterung für Microsoft Visual Studio. Sie soll an ein lokales Profil angehängt werden. AWS Die Richtlinie ermöglicht das Hochladen von Anwendungsartefakten und das Herunterladen der

resultierenden Artefakte von Amazon S3. Es ermöglicht das Erstellen von Anwendungen in einem Container-Image mithilfe AWS CodeBuild und Speichern und Abrufen der Images aus Amazon Elastic Container Registry (Amazon ECR). Und es ermöglicht die Bereitstellung der Anwendung für Container-Services AWS wie Amazon Elastic Container Service (Amazon ECS), die optionale Erstellung von VPC-Ressourcen, die optionale Verbindung zu vorhandener Infrastruktur wie AWS Directory Service und andere verwandte Dienste.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSRefactoringToolkitFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2022, 16:41 UTC
- Zeit bearbeitet: 18. November 2023, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "App2ContainerAccess",
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
```

```
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Sid" : "CodeBuildCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "CodeBuildExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
```

```
    {
      "Sid" : "CreateSecurityGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2CreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2CreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2ModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2ModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcrCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcrModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcsCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcsModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsReadTaskDefinitionAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EcsExecuteCommandInSidecar",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Sid" : "EcsExecuteCommandInSidecarATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Sid" : "CreateEcsServiceLinkedRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
    {
      "Sid" : "CloudwatchCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
    },
    {
      "Sid" : "CloudwatchGetAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "CloudwatchGetAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "SsmParameterAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
```

```
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetECSSLR",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Sid" : "PortingAssistantFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
    {
      "Sid" : "ApplicationTransformationAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
```

```
        }
      }
    },
    {
      "Sid" : "EcrPushAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrAuthAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRefactoringToolkitSidecarPolicy

`AWSRefactoringToolkitSidecarPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie soll von Amazon ECS Tasks verwendet werden, die zum Testen von AnwendungenAWS unter Verwendung derAWS Toolkit for.NET Refactoring-Erweiterung für Microsoft Visual Studio erstellt wurden. Die Richtlinie gewährt Zugriff auf das Herunterladen von Anwendungsartefakten von Amazon S3, die Übermittlung des Status der Aufgabe mithilfe vonAWS Systems Manager und andere erforderliche Dienste.

Verwenden dieser -Richtlinie

Sie können`AWSRefactoringToolkitSidecarPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. Oktober 2022, 16:41 UTC
- Bearbeitete Zeit: 29. Oktober 2022, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit

AWSrePostPrivateCloudWatchAccess

`AWSrePostPrivateCloudWatchAccess`ist eine AWSverwaltete Richtlinie, die: re:POST Private-Zugriff zur Veröffentlichung CloudWatch von Metrikdaten gewährt

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2023, 16:37 UTC
- Bearbeitete Zeit: 15. November 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPublishMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/rePostPrivate",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRepostSpaceSupportOperationsPolicy

`AWSRepostSpaceSupportOperationsPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es dem re:POST Space-Dienst, Supportanfragen zu erstellen, zu verwalten und zu lösen, die über die Space-Anwendung erstellt wurden.

Diese Richtlinie verwenden

Sie können Verbindungen `AWSRepostSpaceSupportOperationsPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. November 2023, 21:52 UTC
- Bearbeitete Zeit: 26. November 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResilienceHubAsssessmentExecutionPolicy

`AWSResilienceHubAsssessmentExecutionPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie für die AWS Resilience Hub-Dienstrolle, die den Zugriff auf andere AWS Dienste ermöglicht, um die Bewertung durchzuführen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResilienceHubAsssessmentExecutionPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 12:32 UTC
- Bearbeitete Zeit: 29. Oktober 2023, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
```

```
            "ec2:DescribePlacementGroups",
            "ec2:DescribeRegions",
            "ec2:DescribeSnapshots",
            "ec2:DescribeSubnets",
            "ec2:DescribeTags",
            "ec2:DescribeVolumes",
            "ec2:DescribeVpcEndpoints",
            "ecr:DescribeRegistry",
            "ecs:DescribeCapacityProviders",
            "ecs:DescribeClusters",
            "ecs:DescribeContainerInstances",
            "ecs:DescribeServices",
            "ecs:DescribeTaskDefinition",
            "ecs:ListContainerInstances",
            "ecs:ListServices",
            "eks:DescribeCluster",
            "eks:DescribeFargateProfile",
            "eks:DescribeNodegroup",
            "eks:ListFargateProfiles",
            "eks:ListNodegroups",
            "elasticache:DescribeCacheClusters",
            "elasticache:DescribeGlobalReplicationGroups",
            "elasticache:DescribeReplicationGroups",
            "elasticache:DescribeSnapshots",
            "elasticfilesystem:DescribeFileSystems",
            "elasticfilesystem:DescribeLifecycleConfiguration",
            "elasticfilesystem:DescribeMountTargets",
            "elasticfilesystem:DescribeReplicationConfigurations",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeTargetGroups",
            "elasticloadbalancing:DescribeTargetHealth",
            "fis:GetExperimentTemplate",
            "fis:ListExperimentTemplates",
            "fis:ListExperiments",
            "lambda:GetFunctionConcurrency",
            "lambda:GetFunctionConfiguration",
            "lambda:ListAliases",
            "lambda:ListVersionsByFunction",
            "rds:DescribeDBClusterSnapshots",
            "rds:DescribeDBClusters",
            "rds:DescribeDBInstanceAutomatedBackups",
            "rds:DescribeDBInstances",
            "rds:DescribeDBProxies",
            "rds:DescribeDBProxyTargets",
```

```
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "s3:GetBucketLocation",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
```

```
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3Statement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*"
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerFullAccess

`AWSResourceAccessManagerFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Resource Access Manager bietet

Verwenden dieser -Richtlinie

Sie können`AWSResourceAccessManagerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. Juni 2019, 17:28 UTC
- Bearbeitete Zeit: 4. Juni 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSResourceAccessManagerReadOnlyAccess

`AWSResourceAccessManagerReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS Resource Access Manager bereitstellt.

Verwenden dieser Richtlinie

Sie können`AWSResourceAccessManagerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Dezember 2019, 20:58 UTC
- Bearbeitete Zeit: 9. Dezember 2019, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSResourceAccessManagerResourceShareParticipantAccess

`AWSResourceAccessManagerResourceShareParticipantAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff aufAWS Resource Access Manager Manager-APIs bietet, die ein Resource Share-Teilnehmer benötigt.

Verwenden dieser Richtlinien

Sie könnenAWSResourceAccessManagerResourceShareParticipantAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Dezember 2019, 20:41 UTC
- Bearbeitete Zeit: 9. Dezember 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSResourceAccessManagerServiceRolePolicy

`AWSResourceAccessManagerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die den schreibgeschütztenAWS Resource Access Manager Manager-Zugriff auf die Organisationsstruktur des Kunden enthält. Sie enthält auch IAM-Berechtigungen für das eigenständige Löschen der Rolle.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 14. November 2018, 19:28 UTC
- Bearbeitete Zeit: 14. November 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSResourceExplorerFullAccess

`AWSResourceExplorerFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Administratorberechtigungen für den Zugriff auf Resource Explorer-Ressourcen und gewährt anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceExplorerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. November 2022, 20:01 UTC
- Bearbeitete Zeit: 14. November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerOrganizationsAccess

`AWSResourceExplorerOrganizationsAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Resource Explorer Administratorberechtigungen und anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen. Der AWS Organisationsadministrator

benötigt diese Berechtigungen, um die Suche mit mehreren Konten in der Konsole einzurichten und zu verwalten.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSResourceExplorerOrganizationsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. November 2023, 17:01 UTC
- Bearbeitete Zeit: 14. November 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerReadOnlyAccess

`AWSResourceExplorerReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt nur Leseberechtigungen zum Suchen und Anzeigen von Resource Explorer-Ressourcen und gewährt anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceExplorerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. November 2022, 19:56 UTC
- Bearbeitete Zeit: 14. November 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerServiceRolePolicy

`AWSResourceExplorerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Resource Explorer ermöglicht, Ressourcen und CloudTrail Ereignisse in Ihrem Namen anzuzeigen, um Ihre Ressourcen für die Suche zu indizieren.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Oktober 2022, 20:35 UTC
- Bearbeitete Zeit: 20. Dezember 2023, 13:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceGroupsReadOnlyAccess

`AWSResourceGroupsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Dies ist die schreibgeschützten Richtlinien fürAWS Resource Groups

Verwenden dieser Richtlinie

Sie können`AWSResourceGroupsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. März 2018, 10:27 UTC
- Bearbeitete Zeit: 5. Februar 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSRoboMaker_FullAccess

`AWSRoboMaker_FullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS RoboMaker über dasAWS Management Console und SDK bietet. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, IAM).

Verwenden dieser -Richtlinie

Sie können`AWSRoboMaker_FullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Erstellungszeit: 10. September 2020, 18:34 UTC
- Bearbeitete Zeit: 16. September 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSRoboMakerReadOnlyAccess

`AWSRoboMakerReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die:AWS RoboMaker Über dasAWS Management Console und SDK nur Lesezugriff gewährt

Verwenden dieser -Richtlinie

Sie können`AWSRoboMakerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. November 2018, 05:30 UTC
- Bearbeitete Zeit: 28. August 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSRoboMakerServicePolicy

`AWSRoboMakerServicePolicy`ist eine AWSverwaltete Richtlinie, die: RoboMaker Servicerichtlinie

Verwenden Sie diese Richtlinie Verwenden diese Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. November 2018, 06:30 UTC
- Bearbeitete Zeit: 11. November 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die Standardversion der Richtlinie ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JAM-Richtliniendokument

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf die geringsten Berechtigungen

AWSRoboMakerServiceRolePolicy

`AWSRoboMakerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: RoboMaker Servicerichtlinie

Verwenden dieser Richtlinie

Sie können`AWSRoboMakerServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. November 2018, 05:33 UTC
- Bearbeitete Zeit: 26. November 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSRolesAnywhereServicePolicy

`AWSRolesAnywhereServicePolicy`ist eine AWSverwaltete Richtlinie, die: Es IAM Roles Anywhere ermöglicht, Service/Nutzungsmetriken für private Zertifizierungsstellen zu veröffentlichen CloudWatch und deren Status in Ihrem Namen zu überprüfen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 5. Juli 2022, 15:26 UTC
- Bearbeitete Zeit: 5. Juli 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien

AWSS3OnOutpostsServiceRolePolicy

`AWSS3OnOutpostsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Erlaubt dem Amazon S3 on Outposts-Service, EC2-Netzwerkressourcen in Ihrem Namen zu verwalten.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Oktober 2023, 20:32 UTC
- Bearbeitete Zeit: 3. Oktober 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSavingsPlansFullAccess

`AWSSavingsPlansFullAccess`ist eine AWSverwaltete Police, die: vollen Zugriff auf den Sparplans-Service bietet

Verwenden dieser -Richtlinie

Sie können`AWSSavingsPlansFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. November 2019, 22:45 UTC
- Bearbeitete Zeit: 6. November 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSavingsPlansReadOnlyAccess

`AWSSavingsPlansReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf den Sparplans-Service bietet

Verwenden dieser -Richtlinie

Sie können`AWSSavingsPlansReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. November 2019, 22:45 UTC
- Bearbeitete Zeit: 6. November 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSecurityHubFullAccess

`AWSSecurityHubFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die Nutzung von AWS Security Hub bietet.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSecurityHubFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 23:54 UTC
- Bearbeitete Zeit: 16. November 2023, 21:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
```

```
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "inspector2:BatchGetAccountStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubOrganizationsAccess

`AWSSecurityHubOrganizationsAccess`ist eine AWSverwaltete Richtlinie, die: Erteilt die Erlaubnis, AWS Security Hub innerhalb einer Organisation zu aktivieren und zu verwalten.

Beinhaltet die unternehmensweite Aktivierung des Dienstes und die Festlegung des delegierten Administratorkontos für den Dienst.

Verwendung dieser Richtlinie

Sie können Verbindungen `AWSSecurityHubOrganizationsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. März 2021, 20:53 UTC
- Bearbeitete Zeit: 16. November 2023, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubReadOnlyAccess

`AWSSecurityHubReadOnlyAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf AWS Security Hub-Ressourcen

Verwenden dieser Richtlinie

Sie können `AWSSecurityHubReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 01:34 UTC
- Bearbeitungszeit: 22. Februar 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSecurityHubServiceRolePolicy

`AWSSecurityHubServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Eine dienstbezogene Rolle, die AWS Security Hub benötigt, um auf Ihre Ressourcen zugreifen zu können.

Diese Richtlinie verwenden

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. November 2018, 23:47 UTC
- Bearbeitete Zeit: 27. November 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "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"
          ]
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAdminFullAccess

`AWSServiceCatalogAdminFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf die Verwaltungsfunktionen des Servicekatalogs bietet

Verwenden dieser -Richtlinie

Sie können`AWSServiceCatalogAdminFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Februar 2018, 17:19 UTC
- Bearbeitete Zeit: 13. April 2023, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceCatalogAdminReadOnlyAccess

`AWSServiceCatalogAdminReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Service Catalog-Administratorfunktionen bietet

Verwenden dieser -Richtlinie

Sie könnenAWSServiceCatalogAdminReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. Oktober 2019, 18:53 UTC
- Bearbeitete Zeit: 25. Oktober 2019, 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalRichtlinien und Umstellung auf Berechtigungen

AWSServiceCatalogAppRegistryFullAccess

`AWSServiceCatalogAppRegistryFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf die Funktionen der Service Catalog App Registry bietet

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSServiceCatalogAppRegistryFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. November 2020, 22:25 UTC
- Bearbeitete Zeit: 7. Dezember 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAppRegistryReadOnlyAccess

`AWSServiceCatalogAppRegistryReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Schreibgeschützten Zugriff auf die Funktionen von Service Catalog App Registry bietet

Verwenden dieser -diese -Richtlinie

Sie können`AWSServiceCatalogAppRegistryReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 12. November 2020, 22:34 UTC
- Bearbeitete Zeit: 17. November 2022, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Standardrichtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceCatalogAppRegistryServiceRolePolicy

`AWSServiceCatalogAppRegistryServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Service Catalog AppRegistry die Verwaltung von Resource Groups in Ihrem Namen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. Mai 2021, 22:18 UTC

- Bearbeitete Zeit: 26. Oktober 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceCatalogEndUserFullAccess

`AWSServiceCatalogEndUserFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf die Funktionen des Servicekatalogs für Endbenutzer bietet

Verwenden dieser -Richtlinie

Sie können`AWSServiceCatalogEndUserFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. Februar 2018, 17:22 UTC
- Bearbeitete Zeit: 10. Juli 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Richtlinie ist die -Richtlinie, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSServiceCatalogEndUserReadOnlyAccess

`AWSServiceCatalogEndUserReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Service Catalog-Endbenutzerfunktionen bietet

Verwenden dieser -Richtlinie

Sie können`AWSServiceCatalogEndUserReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 25. Oktober 2019, 18:49 UTC
- Bearbeitete Zeit: 25. Oktober 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Berechtigungen mit den geringsten Berechtigungen

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Eine Service Linked Role PolicyAWS ServiceCatalog zur Synchronisierung mit derAWS Organisationsstruktur einer Organisation

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 10. April 2023, 20:48 UTC
- Bearbeitete Zeit: 10. April 2023, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinien ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON--Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceCatalogSyncServiceRolePolicy

`AWSServiceCatalogSyncServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Eine Service Linked RoleAWS ServiceCatalog zum Synchronisieren von Provisioning Artifacts aus Quell-Repositorys

Verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die servicegebundene Rolle angehängt, die die servicegebundene Rolle angehängt, die die servicegebundene Rolle angehängt, die die Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 15. November 2022, 21:20 UTC

- Bearbeitete Zeit: 15. November 2022, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtliniendokument Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "ValidateTemplate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS

AWSServiceRoleForAmazonEKSNodegroup

`AWSServiceRoleForAmazonEKSNodegroup` ist eine -AWSverwaltete Richtlinie, die: Erforderliche Berechtigungen für die Verwaltung von Knotengruppen im Kundenkonto. Diese Richtlinien beziehen sich auf die Verwaltung der folgenden Ressourcen: AutoscalingGroups, SecurityGroups LaunchTemplates und InstanceProfiles.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 07. November 2019, 01:34 UTC
- Bearbeitungszeit: 04. Januar 2024, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Richtlinienversion

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff auf Systems Manager Manager-Ressourcen bietet, die von CloudWatch Alarms verwendet werden

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 1. Oktober 2020, 09:49 UTC
- Bearbeitete Zeit: 01. Oktober 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinien

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`ist einAWSverwaltete Richtliniedas: Erlaubt CloudWatch um in Ihrem Namen auf RDS Performance Insights-Metriken zuzugreifen

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Zeitpunkt der Erstellung: 7. September 2023, 09:32 Uhr UTC
- Bearbeitete Zeit:7. September 2023, 09:32 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie: v1(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCodeGuru-Profiler

`AWSServiceRoleForCodeGuru-Profiler`ist eine AWSverwaltete Richtlinie, die: Eine mit einem Service verknüpfte Rolle ist erforderlich, damit Amazon CodeGuru Profiler Benachrichtigungen in Ihrem Namen senden kann.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. Juni 2020, 22:04 UTC
- Bearbeitete Zeit: 26. Juni 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceRoleForCodeWhispererPolicy

`AWSServiceRoleForCodeWhispererPolicy` ist eine -AWS verwaltete Richtlinie, die: Diese Rolle gewährt Berechtigungen für den Zugriff CodeWhisperer auf Daten in Ihrem Konto, um die Abrechnung zu berechnen, bietet Zugriff zum Erstellen und Zugreifen auf Sicherheitsberichte in Amazon CodeGuruund gibt Daten an aus CloudWatch.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 24. März 2023, 19:39 UTC

- Bearbeitungszeit: 01. März 2024, 23:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Richtlinienversion

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid4",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:GetFindings"
      ],
      "Resource" : [
        "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
      ]
    },
    {
      "Sid" : "sid5",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/CodeWhisperer"
          ]
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSServiceRoleForEC2ScheduledInstances

`AWSServiceRoleForEC2ScheduledInstances`ist eine AWSverwaltete Richtlinie, die: Es EC2 Scheduled Instances ermöglicht, Spot-Instances zu starten und zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. Oktober 2017, 18:31 UTC
- Bearbeitete Zeit: 12. Oktober 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`ist eine AWSverwaltete Richtlinie, die: diese dienstverknüpfte RolleAWS GroundStation verwendet, um EC2 aufzurufen, um öffentliche IPv4-Adressen zu finden

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 13. Dezember 2022, 23:52 UTC
- Bearbeitete Zeit: 13. Dezember 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceRoleForImageBuilder

`AWSServiceRoleForImageBuilder`ist eine AWSverwaltete Richtlinie, die: EC2 ImageBuilder ermöglicht, AWS Dienste in Ihrem Namen aufzurufen.

Verwenden Sie diese Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2019, 22:02 UTC
- Bearbeitete Zeit: 19. Oktober 2023, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Version der Richtlinie

Richtlinienversion: v19 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForIoTSiteWise

`AWSServiceRoleForIoTSiteWise`ist eine AWSverwaltete Richtlinie, die: AWS IoT SiteWise die Bereitstellung und Verwaltung von Gateways sowie die Abfrage von Daten ermöglicht. Die Richtlinie umfasst die erforderlichen AWS Greengrass-Berechtigungen für die Bereitstellung in Gruppen, AWS Lambda-Berechtigungen für die Erstellung und Aktualisierung von Funktionen mit Servicepräfix und AWS IoT Analytics Analytics-Berechtigungen für die Abfrage von Daten aus Datenspeichern.

Verwenden dieser Richtlinie

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2018, 19:19 UTC
- Bearbeitete Zeit: 13. November 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForLogDeliveryPolicy

`AWSServiceRoleForLogDeliveryPolicy`ist eine AWSverwaltete Richtlinie, die: Ermöglicht dem Log Delivery Service die Übermittlung von Protokollen, indem er die Protokolladresse in Ihrem Namen aufruft.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 4. Oktober 2019, 17:31 UTC
- Bearbeitete Zeit: 15. Juli 2021, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die die die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceRoleForMonitronPolicy

`AWSServiceRoleForMonitronPolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Monitron Berechtigungen zur Verwaltung vonAWS Ressourcen gewährt, einschließlich derAWS SSO-Benutzerzuweisung in Ihrem Namen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 2. Dezember 2020, 19:06 UTC

- Bearbeitete Zeit: 29. September 2022, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceRoleForNeptuneGraphPolicy

`AWSServiceRoleForNeptuneGraphPolicy`ist eine AWSverwaltete Richtlinie, die: Cloudwatch-Zugriff zur Veröffentlichung von Betriebs- und Nutzungsmetriken und Protokollen für Amazon Neptune bietet

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2023, 14:03 UTC
- Bearbeitete Zeit: 29. November 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForPrivateMarketplaceAdminPolicy

`AWSServiceRoleForPrivateMarketplaceAdminPolicy` ist eine von AWS verwaltete Richtlinie, die: Bietet Berechtigungen zum Beschreiben und Aktualisieren von Private Marketplace-Ressourcen und zum Beschreiben von AWS Organizations

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 14. Februar 2024, 22:28 UTC
- Bearbeitungszeit: 14. Februar 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Richtlinienversion

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSServiceRoleForSMS

`AWSServiceRoleForSMS`ist eine AWSverwaltete Richtlinie, die: Zugriff aufAWS Dienste und Ressourcen bietet, die für die Migration von Service-Instanzen erforderlich sind,AWS einschließlich EC2, S3 und Cloudformation.

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 6. August 2019, 18:39 UTC
- Bearbeitete Zeit: 15. Oktober 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Version der Richtlinie

Version der Richtlinie:v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceRolePolicyForBackupReports

`AWSServiceRolePolicyForBackupReports`ist eine AWSverwaltete Richtlinie, die:AWS Backup-Berechtigungen zur Erstellung von Compliance-Berichten in Ihrem Namen bereitstellt

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. August 2021, 21:16 UTC
- Bearbeitete Zeit: 10. März 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die -Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSServiceRolePolicyForBackupRestoreTesting

`AWSServiceRolePolicyForBackupRestoreTesting` ist eine von AWS verwaltete Richtlinie, die: Diese Richtlinie enthält Berechtigungen zum Testen von Wiederherstellungen und zum Bereinigen von Ressourcen, die während Tests erstellt wurden.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 10. November 2023, 23:37 UTC
- Bearbeitungszeit: 14. Februar 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSShieldDRTAccessPolicy

`AWSShieldDRTAccessPolicy`ist eine AWSverwaltete Richtlinie, die: DemAWS DDoS-Response-Team eingeschränkten Zugriff auf Ihre Daten gewährt,AWS-Konto um Sie bei der Abwehr von DDoS-Angriffen bei einem schwerwiegenden Ereignis zu unterstützen.

Verwenden dieser Richtlinie

Sie können`AWSShieldDRTAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 5. Juni 2018, 22:29 UTC
- Bearbeitete Zeit: 15. Dezember 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSShieldServiceRolePolicy

`AWSShieldServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Shield den Zugriff aufAWS Ressourcen in Ihrem Namen ermöglicht, um DDoS-Schutz zu bieten.

Verwenden von Richtlinien

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die servicegebundene Rolle angehängt ist, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. November 2021, 19:17 UTC
- Bearbeitete Zeit: 17. November 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

J------

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
```

```
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS mit -Richtlinien und Umstellung auf Berechtigungen

AWSSSMForSAPServiceLinkedRolePolicy

`AWSSSMForSAPServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: AWS Systems Manager for SAP mit den Berechtigungen ausstattet, die für die Verwaltung und Integration von SAP-Software erforderlich sindAWS.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. November 2022, 01:18 UTC
- Bearbeitete Zeit: 21. November 2023, 03:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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_*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSMOpsInsightsServiceRolePolicy

`AWSSSMOpsInsightsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie für Service Linked Role AWSServiceRoleForAmazonSSM_OpsInsights

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 16. Juni 2021, 20:12 UTC
- Bearbeitete Zeit: 16. Juni 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die die die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSSODirectoryAdministrator

`AWSSSODirectoryAdministrator`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff für das SSO-Verzeichnis

Verwenden dieser -Richtlinie

Sie können`AWSSSODirectoryAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 31. Oktober 2018, 23:54 UTC
- Bearbeitete Zeit: 20. Oktober 2022, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSSODirectoryReadOnly

`AWSSSODirectoryReadOnly`ist eine AWSverwaltete Richtlinie, die: ReadOnly Zugriff auf das SSO-Verzeichnis

Verwenden dieser -Richtlinie

Sie können`AWSSSODirectoryReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 31. Oktober 2018, 23:49 UTC
- Bearbeitete Zeit: 16. November 2022, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Standardrichtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf

eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSSOMasterAccountAdministrator

`AWSSSOMasterAccountAdministrator`ist eine AWSverwaltete Richtlinie, die: Innerhalb vonAWS SSO Zugriff auf die Verwaltung der Master- und Mitgliedskonten sowie der Cloud-Anwendung vonAWS Organizations bietet

Verwenden dieser Richtlinie

Sie können`AWSSSOMasterAccountAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Juni 2018, 20:36 UTC
- Bearbeitete Zeit: 20. Oktober 2022, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSSOMemberAccountAdministrator

`AWSSSOMemberAccountAdministrator`ist eine AWSverwaltete Richtlinie, die: Zugriff innerhalb vonAWS SSO zur Verwaltung der Mitgliedskonten und der Cloud-Anwendung vonAWS Organizations bietet

Verwenden dieser Richtlinie

Sie können`AWSSSOMemberAccountAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Juni 2018, 20:45 UTC
- Bearbeitete Zeit: 20. Oktober 2022, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSSOReadOnly

`AWSSSOReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff aufAWS SSO-Konfigurationen bietet.

Verwenden dieser Richtlinien

Sie können`AWSSSOReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Juni 2018, 20:24 UTC
- Bearbeitete Zeit: 22. August 2022, 17:23 UTC

- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Version der Richtlinie

Version der Richtlinie:v8 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONRichtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSSOServiceRolePolicy

`AWSSSOServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS SSO-Berechtigungen zur Verwaltung vonAWS Ressourcen, einschließlich IAM-Rollen, Richtlinien und SAML-IdP, in Ihrem Namen gewährt.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 5. Dezember 2017, 18:36 UTC
- Bearbeitete Zeit: 20. Oktober 2022, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v17 (Standard)

Die Standardversion der Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSStepFunctionsConsoleFullAccess

`AWSStepFunctionsConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Eine Zugriffsrichtlinie, die einem Benutzer/einer Rolle, usw. den Zugriff auf dieAWS StepFunctions Konsole ermöglicht. Für eine vollständige Konsolenerfahrung benötigt ein Benutzer zusätzlich zu dieser Richtlinie möglicherweise diePassRole Berechtigung iam: für andere IAM-Rollen, die vom Dienst übernommen werden können.

Verwenden dieser Richtlinie

Sie können`AWSStepFunctionsConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Januar 2017, 21:54 UTC
- Bearbeitete Zeit: 12. Januar 2017, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSStepFunctionsFullAccess

`AWSStepFunctionsFullAccess`ist eine AWSverwaltete Richtlinie, die: Eine Zugriffsrichtlinie für den Zugriff eines Benutzers/einer Rolle/usw. auf dieAWS StepFunctions API. Für vollen Zugriff MUSS ein Benutzer zusätzlich zu dieser Richtlinie über die iam:PassRole -Berechtigung für mindestens eine IAM-Rolle verfügen, die vom Dienst übernommen werden kann.

Verwenden dieser -Richtlinie

Sie können`AWSStepFunctionsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Januar 2017, 21:51 UTC
- Bearbeitete Zeit: 11. Januar 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für

den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSStepFunctionsReadOnlyAccess

`AWSStepFunctionsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Eine Zugriffsrichtlinie, um einem Benutzer/einer Rolle/usw. nur Lesezugriff auf denAWS StepFunctions Dienst zu gewähren.

Verwenden dieser -Richtlinie

Sie können`AWSStepFunctionsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Januar 2017, 21:46 UTC

- Bearbeitete Zeit: 10. November 2017, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSStorageGatewayFullAccess

`AWSStorageGatewayFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff aufAWS Storage Gateway über die bietetAWS Management Console.

Verwenden dieser Richtlinie

Sie können`AWSStorageGatewayFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. September 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSStorageGatewayReadOnlyAccess

`AWSStorageGatewayReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht den Zugriff aufAWS Storage Gateway über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`AWSStorageGatewayReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. September 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalRichtlinien und auf Berechtigungen mit den geringsten Berechtigungen

AWSStorageGatewayServiceRolePolicy

`AWSStorageGatewayServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Die dienstgebundene Rolle wird vonAWS Storage Gateway verwendet, um die Integration andererAWS Dienste mit Storage Gateway zu ermöglichen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. Februar 2021, 19:03 UTC
- Bearbeitete Zeit: 17. Februar 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Richtlinie ist die die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf die geringsten Berechtigungen

AWSSupplyChainFederationAdminAccess

`AWSSupplyChainFederationAdminAccess`ist eine AWSverwaltete Richtlinie,
die: Supply-Chain-Verbundbenutzern Zugriff auf die AWS Supply Chain-Anwendung AWSSupplyChainFederationAdminAccess gewährtAWS, einschließlich der erforderlichen Berechtigungen, um Aktionen innerhalb der AWS Supply Chain-Anwendung auszuführen. Die Richtlinie gewährt Administratorberechtigungen für Benutzer und Gruppen von IAM Identity Center und ist einer Rolle zugeordnet, die von AWS Supply Chain in Ihrem Namen erstellt wurde. Sie sollten keine AWSSupplyChainFederationAdminAccess Richtlinie an andere IAM-Entitäten anhängen.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `AWSSupplyChainFederationAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. März 2023, 18:54 UTC

- Bearbeitete Zeit: 1. November 2023, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportAccess

`AWSSupportAccess`ist eine AWSverwaltete Richtlinie, die: Benutzern den Zugriff auf dasAWS Support Center ermöglicht.

Verwenden dieser Richtlinien

Sie können`AWSSupportAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die Berechtigungen definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

AWSSupportAppFullAccess

`AWSSupportAppFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf dieAWS Support App und andere erforderliche Dienste wieAWS Support Service Quotas bietet. Diese Richtlinie beinhaltet Berechtigungen zur Nutzung der unterstützenden Dienste, sodass sich der Benutzer beiAWS Support Supportanfragen an ihn wenden, Servicekontingente ändern und die entsprechenden dienstverknüpften Rollen erstellen kann.

Verwenden dieser Richtlinien

Sie können`AWSSupportAppFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. August 2022, 16:53 UTC
- Bearbeitete Zeit: 22. August 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSupportAppReadOnlyAccess

`AWSSupportAppReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf dieAWS Support App bietet.

Verwenden dieser -Richtlinie

Sie könnenAWSSupportAppReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. August 2022, 17:01 UTC
- Bearbeitete Zeit: 22. August 2022, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSSupportPlansFullAccess

`AWSSupportPlansFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Supportpläne bietet.

Verwenden dieser -Richtlinie

Sie können`AWSSupportPlansFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. September 2022, 18:19 UTC
- Bearbeitete Zeit: 9. Mai 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der -Richtlinie definiert, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

Dokument mit JSONet-Richtlinie

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinie IAM-Richtlinie mit IAM-Richtlinie
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete verwaltete verwaltete -verwaltete verwaltete verwaltete verwaltete verwaltete verwaltete verwaltete verwaltete

AWSSupportPlansReadOnlyAccess

`AWSSupportPlansReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Supportpläne gewährt.

Verwenden dieser -Richtlinie

Sie können`AWSSupportPlansReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. September 2022, 18:08 UTC
- Bearbeitete Zeit: 27. September 2022, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSupportServiceRolePolicy

`AWSSupportServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Ermöglicht AWS Support den Zugriff auf -AWSRessourcen, um Fakturierungs-, Verwaltungs- und Support-Services bereitzustellen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 19. April 2018, 18:04 UTC
- Bearbeitungszeit: 17. Januar 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v34 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
```

```
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
```

```
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActions",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
```

```
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
```

```
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listOperations",
        "apprunner:listServices",
        "apprunner:listTagsForResource",
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
```

```
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listWorkspaces",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
```

```
        "auditmanager:listAssessmentReports",
        "auditmanager:listAssessments",
        "auditmanager:listControls",
        "auditmanager:listKeywordsForDataSource",
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
        "autoscaling:describeTags",
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeWarmPool",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
```

```
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listTags",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "batch:describeComputeEnvironments",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:listJobs",
        "braket:getDevice",
        "braket:getQuantumTask",
        "braket:searchDevices",
        "braket:searchQuantumTasks",
        "budgets:viewBudget",
        "ce:getCostAndUsage",
        "ce:getCostAndUsageWithResources",
        "ce:getCostForecast",
        "ce:getDimensionValues",
        "ce:getReservationCoverage",
        "ce:getReservationPurchaseRecommendation",
```

```
        "ce:getReservationUtilization",
        "ce:getRightsizingRecommendation",
        "ce:getSavingsPlansCoverage",
        "ce:getSavingsPlansPurchaseRecommendation",
        "ce:getSavingsPlansUtilization",
        "ce:getSavingsPlansUtilizationDetails",
        "ce:getTags",
        "chime:describeAppInstance",
        "chime:getAttendee",
        "chime:getGlobalSettings",
        "chime:getMediaCapturePipeline",
        "chime:getMediaPipeline",
        "chime:getMeeting",
        "chime:getProxySession",
        "chime:getSipMediaApplication",
        "chime:getSipRule",
        "chime:getVoiceConnector",
        "chime:getVoiceConnectorGroup",
        "chime:getVoiceConnectorLoggingConfiguration",
        "chime:listAppInstances",
        "chime:listAttendees",
        "chime:listChannelBans",
        "chime:listChannels",
        "chime:listChannelsModeratedByAppInstanceUser",
        "chime:listMediaCapturePipelines",
        "chime:listMediaPipelines",
        "chime:listMeetings",
        "chime:listSipMediaApplications",
        "chime:listSipRules",
        "chime:listVoiceConnectorGroups",
        "chime:listVoiceConnectors",
        "cleanrooms:batchGetCollaborationAnalysisTemplate",
        "cleanrooms:batchGetSchema",
        "cleanrooms:getAnalysisTemplate",
        "cleanrooms:getCollaboration",
        "cleanrooms:getCollaborationAnalysisTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getSchema",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredTableAssociations",
```

```
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listSchemas",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
```

```
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listStreamingDistributions",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
```

```
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
        "codebuild:batchGetBuilds",
        "codebuild:batchGetProjects",
        "codebuild:listBuildBatches",
        "codebuild:listBuildBatchesForProject",
        "codebuild:listBuilds",
        "codebuild:listBuildsForProject",
```

```
        "codebuild:listCuratedEnvironmentImages",
        "codebuild:listProjects",
        "codebuild:listSourceCredentials",
        "codecommit:batchGetRepositories",
        "codecommit:getBranch",
        "codecommit:getRepository",
        "codecommit:getRepositoryTriggers",
        "codecommit:listBranches",
        "codecommit:listRepositories",
        "codedeploy:batchGetApplicationRevisions",
        "codedeploy:batchGetApplications",
        "codedeploy:batchGetDeploymentGroups",
        "codedeploy:batchGetDeploymentInstances",
        "codedeploy:batchGetDeployments",
        "codedeploy:batchGetDeploymentTargets",
        "codedeploy:batchGetOnPremisesInstances",
        "codedeploy:getApplication",
        "codedeploy:getApplicationRevision",
        "codedeploy:getDeployment",
        "codedeploy:getDeploymentConfig",
        "codedeploy:getDeploymentGroup",
        "codedeploy:getDeploymentInstance",
        "codedeploy:getDeploymentTarget",
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listWebhooks",
        "codestar:describeProject",
        "codestar:listProjects",
```

```
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
```

```
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
```

```
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
```

```
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getHomeRegion",
        "controltower:getLandingZoneStatus",
        "controltower:listDirectoryGroups",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listManagedAccounts",
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
```

```
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
        "devicefarm:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
        "devicefarm:listJobs",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
```

```
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEventCategories",
        "dms:describeEvents",
        "dms:describeEventSubscriptions",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstances",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "docdb-elastic:getCluster",
        "docdb-elastic:getClusterSnapshot",
```

```
        "docdb-elastic:listClusters",
        "docdb-elastic:listClusterSnapshots",
        "drs:describeJobLogItems",
        "drs:describeJobs",
        "drs:describeLaunchConfigurationTemplates",
        "drs:describeRecoveryInstances",
        "drs:describeRecoverySnapshots",
        "drs:describeReplicationConfigurationTemplates",
        "drs:describeSourceNetworks",
        "drs:describeSourceServers",
        "drs:getLaunchConfiguration",
        "drs:getReplicationConfiguration",
        "drs:listExtensibleSourceServers",
        "drs:listLaunchActions",
        "drs:listStagingAccounts",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTimeToLive",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
```

```
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
```

```
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
```

```
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
```

```
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImages",
        "ecr:describeImageReplicationStatus",
```

```
        "ecr:describeImageScanFindings",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:listImages",
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
```

```
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
```

```
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
```

```
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
        "elastictranscoder:readPreset",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
```

```
        "es:listVpcEndpointsForDomain",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
        "evidently:listSegments",
        "evidently:listSegmentReferences",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listArchives",
        "events:listApiDestinations",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fms:getAdminAccount",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:listComplianceStatus",
        "fms:listMemberAccounts",
        "fms:listPolicies",
```

```
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
        "forecast:listForecasts",
        "forecast:listPredictors",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
```

```
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
```

```
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
```

```
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:querySchemaVersionMetadata",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listDeployments",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
        "greengrass:listSubscriptionDefinitionVersions",
```

```
        "guardduty:getDetector",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMasterAccount",
        "guardduty:getMembers",
        "guardduty:getThreatIntelSet",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
```

```
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
```

```
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflowStepExecutions",
        "imagebuilder:listTagsForResource",
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "inspector-scan:scanSbom",
```

```
        "internetmonitor:getMonitor",
        "internetmonitor:listMonitors",
        "internetmonitor:getHealthEvent",
        "internetmonitor:listHealthEvents",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
        "iot:getIndexingConfiguration",
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
```

```
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
        "iotevents:listDetectors",
        "iotevents:listInputs",
        "iotfleetwise:getCampaign",
        "iotfleetwise:getDecoderManifest",
        "iotfleetwise:getFleet",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getVehicle",
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifests",
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listVehicles",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
```

```
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
        "iottwinmaker:getScene",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
        "iottwinmaker:getSyncJob",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
```

```
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:getBootstrapBrokers",
        "kafka:listConfigurations",
        "kafka:listConfigurationRevisions",
        "kafka:listClusterOperations",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listNodes",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeDataSource",
        "kendra:describeFaq",
        "kendra:describeIndex",
        "kendra:listDataSources",
        "kendra:listFaqs",
        "kendra:listIndices",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreams",
        "kinesis:listStreamConsumers",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisvideo:describeImageGenerationConfiguration",
```

```
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listStreams",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
```

```
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
        "lex:describeCustomVocabularyMetadata",
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
        "lex:getBotChannelAssociation",
        "lex:getBotChannelAssociations",
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager:getLicenseConfiguration",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
```

```
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listResourceInventory",
        "license-manager:listUsageForLicenseConfiguration",
        "lightsail:getActiveNames",
        "lightsail:getAlarms",
        "lightsail:getAutoSnapshots",
        "lightsail:getBlueprints",
        "lightsail:getBucketBundles",
        "lightsail:getBucketMetricData",
        "lightsail:getBuckets",
        "lightsail:getBundles",
        "lightsail:getCertificates",
        "lightsail:getContainerImages",
        "lightsail:getContainerServiceDeployments",
        "lightsail:getContainerServiceMetricData",
        "lightsail:getContainerServicePowers",
        "lightsail:getContainerServices",
        "lightsail:getDisk",
        "lightsail:getDisks",
        "lightsail:getDiskSnapshot",
        "lightsail:getDiskSnapshots",
        "lightsail:getDistributionBundles",
        "lightsail:getDistributionMetricData",
        "lightsail:getDistributions",
        "lightsail:getDomain",
        "lightsail:getDomains",
        "lightsail:getExportSnapshotRecords",
        "lightsail:getInstance",
        "lightsail:getInstanceMetricData",
        "lightsail:getInstancePortStates",
        "lightsail:getInstances",
        "lightsail:getInstanceSnapshot",
        "lightsail:getInstanceSnapshots",
        "lightsail:getInstanceState",
        "lightsail:getKeyPair",
        "lightsail:getKeyPairs",
        "lightsail:getLoadBalancer",
        "lightsail:getLoadBalancerMetricData",
        "lightsail:getLoadBalancers",
        "lightsail:getLoadBalancerTlsCertificates",
        "lightsail:getOperation",
        "lightsail:getOperations",
```

```
        "lightsail:getOperationsForResource",
        "lightsail:getRegions",
        "lightsail:getRelationalDatabase",
        "lightsail:getRelationalDatabaseMetricData",
        "lightsail:getRelationalDatabases",
        "lightsail:getRelationalDatabaseSnapshot",
        "lightsail:getRelationalDatabaseSnapshots",
        "lightsail:getStaticIp",
        "lightsail:getStaticIps",
        "lightsail:isVpcPeered",
        "logs:describeAccountPolicies",
        "logs:describeDeliveries",
        "logs:describeDeliveryDestinations",
        "logs:describeDeliverySources",
        "logs:describeDestinations",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:listLogDeliveries",
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "lookoutmetrics:describeAlert",
        "lookoutmetrics:describeAnomalyDetectionExecutions",
        "lookoutmetrics:describeAnomalyDetector",
```

```
        "lookoutmetrics:describeMetricSet",
        "lookoutmetrics:getAnomalyGroup",
        "lookoutmetrics:getDataQualityMetrics",
        "lookoutmetrics:getFeedback",
        "lookoutmetrics:getSampleData",
        "lookoutmetrics:listAlerts",
        "lookoutmetrics:listAnomalyDetectors",
        "lookoutmetrics:listAnomalyGroupSummaries",
        "lookoutmetrics:listAnomalyGroupTimeSeries",
        "lookoutmetrics:listMetricSets",
        "lookoutmetrics:listTagsForResource",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:getClassificationExportConfiguration",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingStatistics",
        "macie2:listClassificationJobs",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "managedblockchain:getMember",
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
```

```
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:listChannels",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
```

```
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
```

```
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
        "networkmanager:describeGlobalNetworks",
        "networkmanager:getConnectAttachment",
        "networkmanager:getConnections",
        "networkmanager:getConnectPeer",
        "networkmanager:getConnectPeerAssociations",
        "networkmanager:getCoreNetwork",
        "networkmanager:getCoreNetworkChangeEvents",
        "networkmanager:getCoreNetworkChangeSet",
        "networkmanager:getCoreNetworkPolicy",
        "networkmanager:getCustomerGatewayAssociations",
        "networkmanager:getDevices",
        "networkmanager:getLinkAssociations",
        "networkmanager:getLinks",
        "networkmanager:getNetworkResourceCounts",
        "networkmanager:getNetworkResourceRelationships",
        "networkmanager:getNetworkResources",
        "networkmanager:getNetworkRoutes",
        "networkmanager:getNetworkTelemetry",
        "networkmanager:getResourcePolicy",
        "networkmanager:getRouteAnalysis",
        "networkmanager:getSites",
        "networkmanager:getSiteToSiteVpnAttachment",
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
```

```
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "nimble:getEula",
        "nimble:getLaunchProfile",
        "nimble:getLaunchProfileDetails",
        "nimble:getLaunchProfileInitialization",
        "nimble:getLaunchProfileMember",
        "nimble:getStreamingImage",
        "nimble:getStreamingSession",
        "nimble:getStreamingSessionStream",
        "nimble:getStudio",
        "nimble:getStudioComponent",
        "nimble:listEulaAcceptances",
        "nimble:listEulas",
        "nimble:listLaunchProfiles",
        "nimble:listStreamingImages",
        "nimble:listStreamingSessions",
        "nimble:listStudioComponents",
        "nimble:listStudios",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
```

```
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunGroup",
        "omics:getSequenceStore",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferenceStores",
        "omics:listReferences",
        "omics:listRunGroups",
        "omics:listRunTasks",
        "omics:listRuns",
        "omics:listSequenceStores",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
```

```
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:listAccounts",
        "organizations:listTagsForResource",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
```

```
        "personalize:listDatasetExportJobs",
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listRecipes",
        "personalize:listRecommenders",
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworks",
        "private-networks:listNetworkResources",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
```

```
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
```

```
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEvents",
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
```

```
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
```

```
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
```

```
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
```

```
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
```

```
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express:listAllMyDirectoryBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
```

```
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
```

```
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
```

```
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCards",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "savingsplans:describeSavingsPlans",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
```

```
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "securityhub:getEnabledStandards",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securitylake:getDataLakeExceptionSubscription",
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
```

```
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
```

```
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
```

```
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
```

```
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutions",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatches",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
```

```
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocuments",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocumentVersions",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeApplication",
        "sso:describeInstance",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getManagedApplicationInstance",
        "sso:getSharedSsoConfiguration",
```

```
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
```

```
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
```

```
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
        "transfer:describeUser",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
        "transfer:listUsers",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
```

```
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
```

```
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
```

```
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
        "workmail:listResourceDelegates",
        "workmail:listResources",
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSSystemsManagerAccountDiscoveryServicePolicy

`AWSSystemsManagerAccountDiscoveryServicePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Systems Manager (SSM) die Berechtigung erteilt,AWS-Konto Informationen zu ermitteln.

Verwenden dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 24. Oktober 2019, 17:21 UTC
- Bearbeitete Zeit: 17. Oktober 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSystemsManagerChangeManagementServicePolicy

`AWSSystemsManagerChangeManagementServicePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff aufAWS Ressourcen bietet, die vomAWS Systems Manager Change Management Framework verwaltet oder verwendet werden.

Verwenden von diese Richtlinie, die von

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen angehängt sind.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 7. Dezember 2020, 22:21 UTC
- Bearbeitete Zeit: 7. Dezember 2020, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die StandardVersion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen für die geringsten Berechtigungen mit den geringsten Berechtigungen

AWSSystemsManagerForSAPFullAccess

`AWSSystemsManagerForSAPFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf denAWS Systems Manager for SAP-Service bietet

Verwenden dieser Richtlinien

Sie können`AWSSystemsManagerForSAPFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. November 2022, 02:11 UTC
- Bearbeitete Zeit: 18. November 2022, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -verwaltete -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSystemsManagerForSAPReadOnlyAccess

`AWSSystemsManagerForSAPReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf denAWS Systems Manager for SAP-Service gewährt

Verwenden dieser -Richtlinie

Sie können`AWSSystemsManagerForSAPReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 17. November 2022, 02:11 UTC
- Bearbeitete Zeit: 17. November 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
```

```
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSSystemsManagerOpsDataSyncServiceRolePolicy

`AWSSystemsManagerOpsDataSyncServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: IAM-Rolle für SSM Explorer zur Verwaltung OpsData verwandter Operationen

Verwendung dieser Richtlinie

Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen auszuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstverknüpfte Rollen
- Aufnahmezeit: 26. April 2021, 20:42 UTC
- Bearbeitete Zeit: 28. Juni 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

AWSThinkboxAssetServerPolicy

`AWSThinkboxAssetServerPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt demAWS Portal Asset Server die für den normalen Betrieb erforderlichen Berechtigungen.

Verwenden dieser Richtlinie

Sie könnenAWSThinkboxAssetServerPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2020, 19:18 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

AWSThinkboxAWSPortalAdminPolicy

`AWSThinkboxAWSPortalAdminPolicy` ist eine -AWS verwaltete Richtlinie, die: Diese Richtlinie gewährt der -Deadline-Software von AWS thinkbox vollen Zugriff auf mehrere - AWS Services, wie für die AWS Portalverwaltung erforderlich. Dies umfasst den Zugriff auf die Erstellung beliebiger Tags auf mehreren EC2-Ressourcentypen.

Verwenden dieser Richtlinie

Sie können `AWSThinkboxAWSPortalAdminPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:41 UTC
- Bearbeitungszeit: 23. Februar 2024, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Richtlinienversion

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
```

```
    {
      "Sid" : "AWSThinkboxAWSPortal13",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
```

```
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSThinkboxAWSPortalGatewayPolicy

`AWSThinkboxAWSPortalGatewayPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt demAWS Portal Gateway-Computer die für den normalen Betrieb erforderlichen Berechtigungen.

Verwenden dieser Richtlinie

Sie können`AWSThinkboxAWSPortalGatewayPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2020, 19:05 UTC
- Bearbeitete Zeit: 30. Juni 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Funktion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AWSThinkboxAWSPortalWorkerPolicy

`AWSThinkboxAWSPortalWorkerPolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt den Deadline Workers imAWS Portal die für den normalen Betrieb erforderlichen Berechtigungen.

Verwenden dieser -Richtlinie

Sie können`AWSThinkboxAWSPortalWorkerPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2020, 19:15 UTC
- Bearbeitete Zeit: 7. Dezember 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONRichtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSThinkboxDeadlineResourceTrackerAccessPolicy

`AWSThinkboxDeadlineResourceTrackerAccessPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen gewährt, die für den Betrieb des Deadline Resource Tracker vonAWS Thinkbox erforderlich sind. Dies beinhaltet den vollen Zugriff auf einige EC2-Aktionen, einschließlich DeleteFleets und CancelSpotFleetRequests.

Verwenden dieser -Richtlinie

Sie könnenAWSThinkboxDeadlineResourceTrackerAccessPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2020, 19:25 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSThinkboxDeadlineResourceTrackerAdminPolicy

`AWSThinkboxDeadlineResourceTrackerAdminPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen gewährt, die zum Erstellen, Löschen und Verwalten des Deadline Resource Tracker vonAWS Thinkbox erforderlich sind.

Verwenden dieser Richtlinien

Sie können`AWSThinkboxDeadlineResourceTrackerAdminPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2020, 19:29 UTC
- Bearbeitete Zeit: 22. Juni 2022, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker-*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate-*.yaml"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy`ist eine AWSverwaltete Richtlinie, die: Erteilt die erforderlichen Berechtigungen für das Deadline Spot Event Plugin vonAWS Thinkbox. Dazu gehören die Erlaubnis, eine Spot-Flotte anzufordern, zu ändern und zu stornieren, sowie die eingeschränkte PassRole Genehmigung.

Verwenden dieser Richtlinien

Sie könnenAWSThinkboxDeadlineSpotEventPluginAdminPolicy an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2020, 19:38 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete Version ist die -verwaltete Version, die die Berechtigungen für die -verwaltete Richtlinien definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungen gewähren, die für eine EC2-Instance erforderlich sind, auf der dieAWS Thinkbox Deadline Spot Event Plugin Worker-Software ausgeführt wird.

Verwenden dieser Richtlinie

Sie können`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Mai 2020, 19:35 UTC
- Bearbeitete Zeit: 7. Dezember 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -verwalRichtlinien ist die -verwalRichtlinien und definiert die Richtlinien, die Berechtigungen für die Richtlinien. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalRichtlinien und Umstellung auf Berechtigungen

AWSTransferConsoleFullAccess

`AWSTransferConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS Transfer über dieAWS Management Console

Verwenden Sie diese -Richtlinie

Sie können`AWSTransferConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Dezember 2020, 19:33 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete -verwaltete Richtlinien. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSTransferFullAccess

`AWSTransferFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf denAWS Transfer Service bietet.

Verwenden dieser -Richtlinie

Sie können`AWSTransferFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Dezember 2020, 19:37 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 19:37 UTC

- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSTransferLoggingAccess

`AWSTransferLoggingAccess`ist eine AWSverwaltete Richtlinie, die:AWS Transfer vollen Zugriff ermöglicht, um Log-Streams und -Gruppen zu erstellen und Log-Ereignisse Ihrem Konto zuzuordnen

Verwenden dieser Richtlinie

Sie können`AWSTransferLoggingAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 14. Januar 2019, 15:32 UTC
- Bearbeitete Zeit: 14. Januar 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSTransferReadOnlyAccess

`AWSTransferReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff aufAWS Übertragungsdienste bereitstellt.

Verwenden dieser -Richtlinie

Sie können`AWSTransferReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. August 2020, 17:54 UTC
- Bearbeitete Zeit: 27. August 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSTrustedAdvisorPriorityFullAccess

`AWSTrustedAdvisorPriorityFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff aufAWS Trusted Advisor Priority bietet. Diese Richtlinie ermöglicht es dem Benutzer auch, Trusted Advisor als vertrauenswürdigen Dienst mitAWS Organizations hinzuzufügen und delegierten Administratorkonten für die -Priorität festzulegen.

Verwenden dieser Richtlinie

Sie können`AWSTrustedAdvisorPriorityFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 16. August 2022, 16:08 UTC
- Bearbeitete Zeit: 16. August 2022, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSTrustedAdvisorPriorityReadOnlyAccess

`AWSTrustedAdvisorPriorityReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff aufAWS Trusted Advisor Priority gewährt. Dies beinhaltet die Berechtigung, die delegierten Administratorkonten einzusehen.

Verwenden dieser -Richtlinie

Sie können`AWSTrustedAdvisorPriorityReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 16. August 2022, 16:35 UTC
- Bearbeitete Zeit: 16. August 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSTrustedAdvisorReportingServiceRolePolicy

`AWSTrustedAdvisorReportingServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Servicerichtlinie für Trusted Advisor Multiaccount Reporting

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. November 2019, 17:41 UTC
- Bearbeitete Zeit: 28. Februar 2023, 23:23 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSTrustedAdvisorServiceRolePolicy

`AWSTrustedAdvisorServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Zugriff auf den AWS Trusted Advisor Service bietet, um Kosten zu senken, die Leistung zu erhöhen und die Sicherheit Ihrer AWS Umgebung zu verbessern.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 22. Februar 2018, 21:24 UTC
- Bearbeitungszeit: 18. Januar 2024, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

AWSUserNotificationsServiceLinkedRolePolicy

`AWSUserNotificationsServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: EsAWS Benutzerbenachrichtigungen ermöglicht,AWS Dienste in Ihrem Namen anzurufen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 19. April 2023, 13:28 UTC
- Bearbeitete Zeit: 19. April 2023, 13:28 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtdokument

```
{
  "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" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSVendorInsightsAssessorFullAccess

`AWSVendorInsightsAssessorFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf berechtigte Vendor Insights-Ressourcen und die Verwaltung von Vendor Insights-Abonnements bietet

Verwenden dieser Richtlinie

Sie können`AWSVendorInsightsAssessorFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSVendorInsightsAssessorReadOnly

`AWSVendorInsightsAssessorReadOnly`ist eine AWSverwaltete Richtlinie, die: Lesezugriff für die Anzeige berechtigter Vendor Insights-Ressourcen bietet

Verwenden dieser Richtlinie

Sie können`AWSVendorInsightsAssessorReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSVendorInsightsVendorFullAccess

`AWSVendorInsightsVendorFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff für die Erstellung und Verwaltung der Vendor Insights-Ressourcen bietet

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSVendorInsightsVendorFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 19. Oktober 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsVendorReadOnly

`AWSVendorInsightsVendorReadOnly`ist eine AWSverwaltete Richtlinie, die: Lesezugriff für die Anzeige der Vendor Insights-Ressourcen bietet

Verwenden dieser Richtlinie

Sie können`AWSVendorInsightsVendorReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSVpcLatticeServiceRolePolicy

`AWSVpcLatticeServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: VPC Lattice den Zugriff aufAWS Ressourcen in Ihrem Namen ermöglicht.

Verwenden diese Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 30. November 2022, 20:47 UTC
- Bearbeitete Zeit: 30. November 2022, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit denAWS geringsten Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSVPCS2SVpnServiceRolePolicy

`AWSVPCS2SVpnServiceRolePolicy`ist eine AWS-verwaltete Richtlinie, die: Site-to-Site VPN gestatten, Ressourcen im Zusammenhang mit Ihren VPN-Verbindungen zu erstellen und zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 6. August 2019, 14:13 UTC
- Bearbeitete Zeit: 6. August 2019, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSVPCTransitGatewayServiceRolePolicy

`AWSVPCTransitGatewayServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Erlauben Sie VPC Transit Gateway, die erforderlichen Ressourcen für Ihre Transit Gateway Gateway-VPC-Anhänge zu erstellen und zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist einer Servicerolle zugeordnet, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. November 2018, 16:21 UTC
- Bearbeitete Zeit: 15. April 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie definiert die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSVPCVerifiedAccessServiceRolePolicy

`AWSVPCVerifiedAccessServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie zur Aktivierung des AWS Verified Access-Dienstes zur Bereitstellung von Endpunkten in Ihrem Namen

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2022, 03:35 UTC
- Bearbeitete Zeit: 17. November 2023, 21:03 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFConsoleFullAccess

`AWSWAFConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf AWS WAF über dieAWS Management Console. Beachten Sie, dass diese Richtlinie auch Berechtigungen zum Auflisten und Aktualisieren von CloudFront Amazon-Distributionen, Berechtigungen zum Anzeigen von Load Balancern auf AWS Elastic Load Balancing, Berechtigungen zum Anzeigen von Amazon API Gateway Gateway-REST-APIs und -Phasen, Berechtigungen zum Auflisten und Anzeigen von CloudWatch Amazon-Metriken sowie Berechtigungen zum Anzeigen von innerhalb des Kontos aktivierten Regionen gewährt.

Verwenden dieser -Richtlinie

Sie können Verbindungen `AWSWAFConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 6. April 2020, 18:38 UTC
- Bearbeitete Zeit: 05. Juni 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSWAFConsoleReadOnlyAccess

`AWSWAFConsoleReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht schreibgeschützten Zugriff auf AWS WAF über die. AWS Management Console Beachten Sie, dass diese Richtlinie auch Berechtigungen zum Auflisten von CloudFront Amazon-Distributionen, Berechtigungen zum Anzeigen von Load Balancern auf AWS Elastic Load Balancing, Berechtigungen zum Anzeigen von Amazon API Gateway Gateway-REST-APIs und -Phasen, Berechtigungen zum Auflisten und Anzeigen von CloudWatch Amazon-Metriken sowie Berechtigungen zum Anzeigen von innerhalb des Kontos aktivierten Regionen gewährt.

Verwenden dieser -Richtlinie

Sie können Verbindungen `AWSWAFConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 6. April 2020, 18:43 UTC
- Bearbeitete Zeit: 05. Juni 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

AWSWAFFullAccess

`AWSWAFFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf AWS WAF-Aktionen bietet.

Verwenden dieser -Richtlinie

Sie können Verbindungen `AWSWAFFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 06. Oktober 2015, 20:44 UTC
- Bearbeitete Zeit: 05. Juni 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSWAFReadOnlyAccess

`AWSWAFReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf AWS WAF-Aktionen gewährt.

Verwenden dieser -Richtlinie

Sie können Verbindungen `AWSWAFReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 06. Oktober 2015, 20:43 UTC
- Bearbeitete Zeit: 05. Juni 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

AWSWellArchitectedDiscoveryServiceRolePolicy

`AWSWellArchitectedDiscoveryServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Im Namen von Kunden denWellArchitected Zugriff aufAWS Dienste undWellArchitected Ressourcen ermöglicht, die sich auf Ressourcen beziehen.

Verwenden Verwenden Verwenden Verwenden Verwenden Verwenden Verwenden Verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 26. April 2023, 18:36 UTC
- Bearbeitete Zeit: 26. April 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Verwenden SieAWS verwaltete Richtlinien und Verwenden Sie Berechtigungen mit den geringsten Berechtigungen

AWSWellArchitectedOrganizationsServiceRolePolicy

`AWSWellArchitectedOrganizationsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Well-Architected den Zugriff auf Organizations in Ihrem Namen ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 23. Juni 2022, 17:15 UTC

- Bearbeitete Zeit: 25. Juli 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSWickrFullAccess

`AWSWickrFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt dem Wickr-Dienst vollständige Administratorberechtigungen, einschließlich der administrativen Funktionen von Wickr unterAWS Management Console.

Verwenden dieser Richtlinien

Sie können`AWSWickrFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2022, 20:36 UTC
- Bearbeitete Zeit: 27. November 2022, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSXrayCrossAccountSharingConfiguration

`AWSXrayCrossAccountSharingConfiguration`ist eine AWSverwaltete Richtlinie, die: Funktionen zur Verwaltung von Observability Access Manager-Links und zur gemeinsamen Nutzung von X-Ray-Traces bereitstellt

Verwenden dieser -Richtlinie

Sie können`AWSXrayCrossAccountSharingConfiguration` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2022, 13:46 UTC
- Bearbeitete Zeit: 27. November 2022, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSXRayDaemonWriteAccess

`AWSXRayDaemonWriteAccess` ist eine von AWS verwaltete Richtlinie, die: Erlauben Sie dem AWS X-Ray-Daemon, Rohverfolgungssegmentdaten an die API des Services weiterzuleiten und Samplingdaten (Regeln, Ziele usw.) abzurufen, die vom X-Ray-SDK verwendet werden sollen.

Verwenden dieser Richtlinie

Sie können `AWSXRayDaemonWriteAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 28. August 2018, 23:00 UTC
- Bearbeitungszeit: 13. Februar 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSXrayFullAccess

`AWSXrayFullAccess`ist eine AWSverwaltete Richtlinie, die:AWS X-Ray — verwaltete Richtlinie für vollen Zugriff

Verwenden dieser Richtlinie

Sie können`AWSXrayFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2016, 18:30 UTC
- Bearbeitete Zeit: 1. Dezember 2016, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSXrayReadOnlyAccess

`AWSXrayReadOnlyAccess` ist eine -AWS verwaltete Richtlinie, die: AWS X-Ray schreibgeschützt verwaltete Richtlinie

Verwenden dieser Richtlinie

Sie können `AWSXrayReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 01. Dezember 2016, 18:27 UTC
- Bearbeitungszeit: 14. Februar 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSXrayWriteOnlyAccess

`AWSXrayWriteOnlyAccess`ist eine AWSverwaltete Richtlinie, die:AWS X-Ray Write Only Managed Policy

Verwenden dieser Richtlinie

Sie können`AWSXrayWriteOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2016, 18:19 UTC

- Bearbeitete Zeit: 28. August 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie definiert die die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

AWSZonalAutoshiftPracticeRunSLRPolicy

`AWSZonalAutoshiftPracticeRunSLRPolicy`ist eine AWSverwaltete Richtlinie, die: Administratorzugriff für ARC-Zonenschichtübungen und Zugriff auf CloudWatch Alarmstatus zur Überwachung von Übungsläufen bietet.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2023, 17:34 UTC
- Bearbeitete Zeit: 29. November 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

BatchServiceRolePolicy

`BatchServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriff für den AWS Batch-Service gewährt, um die erforderlichen Ressourcen zu verwalten, einschließlich Amazon EC2- und Amazon ECS-Ressourcen.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. März 2021, 06:55 UTC

- Bearbeitete Zeit: 5. Dezember 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Billing

`Billing` ist eine von AWS verwaltete Richtlinie, die: Gewährt Berechtigungen für Fakturierung und Kostenmanagement. Dazu gehören das Anzeigen der Kontonutzung sowie das Anzeigen und Ändern von Budgets und Zahlungsarten.

Verwenden dieser Richtlinie

Sie können `Billing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Richtlinie für Auftragsfunktionen
- Erstellungszeit: 10. November 2016, 17:33 UTC
- Bearbeitungszeit: 17. Januar 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Richtlinienversion

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen

- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

CertificateManagerServiceRolePolicy

`CertificateManagerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die die die die die die von Amazon Certificate Manager ermöglicht.

Verwenden von von von von von von

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 25. Juni 2020, 17:56 UTC
- Bearbeitete Zeit: 25. Juni 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die StandardVersion der Richtlinie ist die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die die Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinien

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter teter teter teter teter teter teter teter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen.

ClientVPNServiceConnectionsRolePolicy

`ClientVPNServiceConnectionsRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, mit derAWS Client VPN Ihre Client-VPN-Endpunktverbindungen verwalten kann.

Verwenden dieser Richtlinie von dieser Richtlinie Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. August 2020, 19:48 UTC
- Bearbeitete Zeit: 12. August 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONSONRichtdokument dokument dokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalpften Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen von Richtlinien mit den geringsten Berechtigungen von Richtlinien Richtlinien Richtlinien

ClientVPNServiceRolePolicy

`ClientVPNServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, mit derAWS Client VPN Ihre Client-VPN-Endpunkte verwalten kann.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen an Ihre Benutzer, Gruppen oder Rollen angehängt haben.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 10. Dezember 2018, 21:20 UTC
- Bearbeitete Zeit: 12. August 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die Standardversion der Richtlinien für die Richtlinie für die Richtlinie für die Richtlinie für die Richtlinie für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument dokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen zu Berechtigungen mit den geringsten Berechtigungen

CloudFormationStackSetsOrgAdminServiceRolePolicy

`CloudFormationStackSetsOrgAdminServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Servicerolle für CloudFormation StackSets (Organisations-Hauptkonto)

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 10. Dezember 2019, 00:20 UTC
- Bearbeitete Zeit: 10. Dezember 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudFormationStackSetsOrgMemberServiceRolePolicy

`CloudFormationStackSetsOrgMemberServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Servicerolle für CloudFormation StackSets (Mitgliedskonto der Organisation)

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 9. Dezember 2019, 23:52 UTC
- Bearbeitete Zeit: 9. Dezember 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudFrontFullAccess

`CloudFrontFullAccess` ist eine -AWSverwaltete Richtlinie, die: Bietet vollen Zugriff auf die CloudFront Konsole und die Möglichkeit, Amazon S3-Buckets über die aufzulistenAWS Management Console.

Verwenden dieser Richtlinie

Sie können `CloudFrontFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. Februar 2015, 18:39 UTC
- Bearbeitungszeit: 04. Januar 2024, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Richtlinienversion

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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::*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

CloudFrontReadOnlyAccess

`CloudFrontReadOnlyAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet Zugriff auf CloudFront Verteilungskonfigurationsinformationen und listet Verteilungen über die aufAWS Management Console.

Verwenden dieser Richtlinie

Sie können `CloudFrontReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. Februar 2015, 18:39 UTC
- Bearbeitungszeit: 04. Januar 2024, 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

CloudHSMServiceRolePolicy

`CloudHSMServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS Ressourcen ermöglicht, die von CloudHSM verwendet oder verwaltet werden

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die die die die die die die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 6. November 2017, 19:12 UTC
- Bearbeitete Zeit: 6. November 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudSearchFullAccess

`CloudSearchFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf den CloudSearch Amazon-Konfigurationsservice bietet.

Verwenden dieser Richtlinie

Sie können`CloudSearchFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion definiert die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudSearchReadOnlyAccess

`CloudSearchReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf den CloudSearch Amazon-Konfigurationsservice bietet.

Verwenden dieser -Richtlinie

Sie können`CloudSearchReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
```

```
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudTrailServiceRolePolicy

`CloudTrailServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Berechtigungsrichtlinie für CloudTrail ServiceLinkedRole

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Oktober 2018, 21:21 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatch-CrossAccountAccess

`CloudWatch-CrossAccountAccess`ist eine AWSverwaltete Richtlinie, die: Es CloudWatch ermöglicht, im Namen des GirokontosCrossAccountSharing Rollen in Remote-Konten zu übernehmen CloudWatch, um Daten konto- und regionsübergreifend anzuzeigen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 23. Juli 2019, 09:59 UTC
- Bearbeitete Zeit: 23. Juli 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONSON-S-SON-

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchActionsEC2Access

`CloudWatchActionsEC2Access`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf CloudWatch Alarme und Metriken sowie EC2-Metadaten bietet. Ermöglicht den Zugriff auf EC2-Instances zum Beenden, Beenden und Neustarten.

Verwenden dieser -Richtlinie

Sie können`CloudWatchActionsEC2Access` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 7. Juli 2015, 00:00 UTC
- Bearbeitete Zeit: 7. Juli 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchAgentAdminPolicy

`CloudWatchAgentAdminPolicy` ist eine -AWSverwaltete Richtlinie, die: Vollständige Berechtigungen, die für die Verwendung von erforderlich sind AmazonCloudWatchAgent.

Verwenden dieser Richtlinie

Sie können `CloudWatchAgentAdminPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 07. März 2018, 00:52 UTC
- Bearbeitungszeit: 05. Februar 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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-*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

CloudWatchAgentServerPolicy

`CloudWatchAgentServerPolicy` ist eine -AWSverwaltete Richtlinie, die: Für die Verwendung von AmazonCloudWatchAgent auf Servern erforderliche Berechtigungen

Verwenden dieser Richtlinie

Sie können `CloudWatchAgentServerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 07. März 2018, 01:06 UTC
- Bearbeitungszeit: 06. Februar 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

CloudWatchApplicationInsightsFullAccess

`CloudWatchApplicationInsightsFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf CloudWatch Application Insights und die erforderlichen Abhängigkeiten bietet.

Verwenden dieser Richtlinie

Sie können`CloudWatchApplicationInsightsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. November 2020, 18:44 UTC
- Bearbeitete Zeit: 25. Januar 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Standardversion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchApplicationInsightsReadOnlyAccess

`CloudWatchApplicationInsightsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf CloudWatch Application Insights gewährt.

Verwenden dieser Richtlinie

Sie können`CloudWatchApplicationInsightsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. November 2020, 18:48 UTC
- Bearbeitete Zeit: 24. November 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste SchritteAWS und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudwatchApplicationInsightsServiceLinkedRolePolicy

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Cloudwatch Application Insights Service Linked Role Policy

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 1. Dezember 2018, 16:22 UTC
- Bearbeitete Zeit: 11. Mai 2023, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v24 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwaltete Richtlinien

CloudWatchApplicationSignalsServiceRolePolicy

`CloudWatchApplicationSignalsServiceRolePolicy` ist eine von AWS verwaltete Richtlinie, die: Richtlinie gewährt CloudWatch Application Signals die Berechtigung, Überwachungs- und Markierungsdaten von anderen relevanten AWS Services zu erfassen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 09. November 2023, 18:09 UTC
- Bearbeitungszeit: 07. März 2024, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchAutomaticDashboardsAccess

`CloudWatchAutomaticDashboardsAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff aufCloudWatch Nicht-APIs bietet, die für die Anzeige CloudWatch automatischer Dashboards verwendet werden, einschließlich des Inhalts von Objekten wie Lambda-Funktionen

Verwenden dieser -Richtlinie

Sie können`CloudWatchAutomaticDashboardsAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. Juli 2019, 10:01 UTC
- Bearbeitete Zeit: 20. April 2021, 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchCrossAccountSharingConfiguration

`CloudWatchCrossAccountSharingConfiguration`ist eine AWSverwaltete Richtlinie, die: Funktionen zur Verwaltung von Observability Access Manager-Links und zur Einrichtung der gemeinsamen Nutzung von CloudWatch Ressourcen bereitstellt

Verwenden dieser -Richtlinie

Sie können`CloudWatchCrossAccountSharingConfiguration` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2022, 14:01 UTC
- Bearbeitete Zeit: 27. November 2022, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchEventsBuiltInTargetExecutionAccess

`CloudWatchEventsBuiltInTargetExecutionAccess`ist eine AWSverwaltete Richtlinie, die: Es integrierten Zielen in Amazon CloudWatch Events ermöglicht, EC2-Aktionen in Ihrem Namen durchzuführen.

Verwenden dieser Richtlinie

Sie können`CloudWatchEventsBuiltInTargetExecutionAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 14. Januar 2016, 18:35 UTC
- Bearbeitete Zeit: 14. Januar 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie definiert die Berechtigungen, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
```

```
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

CloudWatchEventsFullAccess

`CloudWatchEventsFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon CloudWatch Events bietet.

Verwenden dieser -Richtlinie

Sie können`CloudWatchEventsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Januar 2016, 18:37 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchEventsInvocationAccess

`CloudWatchEventsInvocationAccess`ist eine AWSverwaltete Richtlinie, die: Amazon CloudWatch Events erlaubt, Ereignisse an die Streams inAWS Kinesis Streams in Ihrem Konto weiterzuleiten.

Verwenden dieser -Richtlinie

Sie können`CloudWatchEventsInvocationAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 14. Januar 2016, 18:36 UTC
- Bearbeitete Zeit: 14. Januar 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -verwaltete -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchEventsReadOnlyAccess

`CloudWatchEventsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Amazon CloudWatch Events gewährt.

Verwenden dieser -Richtlinie

Sie können`CloudWatchEventsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 14. Januar 2016, 18:27 UTC

- Bearbeitete Zeit: 1. Dezember 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchEventsServiceRolePolicy

`CloudWatchEventsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: ErmöglichtAWS CloudWatch die Ausführung von Aktionen in Ihrem Namen, die durch Alarme und Ereignisse konfiguriert wurden.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die den Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. November 2017 00:42 UTC
- Bearbeitete Zeit: 17. November 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardlinienelement definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchFullAccess

`CloudWatchFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf bietet CloudWatch.

Verwenden dieser Richtlinien

Sie können`CloudWatchFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 27. November 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchFullAccessV2

`CloudWatchFullAccessV2`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf bietet CloudWatch.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchFullAccessV2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. August 2023, 11:32 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchInternetMonitorServiceRolePolicy

`CloudWatchInternetMonitorServiceRolePolicy`ist einAWSverwaltete Richtliniedas: Ermöglicht Internet Monitor den Zugriff auf EC2, Workspaces undCloudFrontRessourcen und andere benötigte Dienste in Ihrem Namen.

Verwendung dieser Richtlinie

Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen auszuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstbezogene Rollen
- Entstehungszeit: 27. November 2022, 17:46 Uhr UTC
- Uhrzeit der Bearbeitung:20. Juli 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie: v2(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eineAWSressource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

CloudWatchLambdaInsightsExecutionRolePolicy

`CloudWatchLambdaInsightsExecutionRolePolicy`ist eine AWSverwaltete Richtlinie, die: Für die Lambda Insights-Erweiterung erforderliche Richtlinie

Verwenden dieser -Richtlinie

Sie können`CloudWatchLambdaInsightsExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 7. Oktober 2020, 19:27 UTC
- Bearbeitete Zeit: 7. Oktober 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -Richtlinie definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchLogsCrossAccountSharingConfiguration

`CloudWatchLogsCrossAccountSharingConfiguration`ist eine AWSverwaltete Richtlinie, die: Funktionen zur Verwaltung von Observability Access Manager-Links und zur Einrichtung der gemeinsamen Nutzung von CloudWatch Logs-Ressourcen bereitstellt

Verwenden dieser -Richtlinie

Sie können`CloudWatchLogsCrossAccountSharingConfiguration` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2022, 13:55 UTC
- Bearbeitete Zeit: 27. November 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchLogsFullAccess

`CloudWatchLogsFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf CloudWatch Protokolle bietet

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchLogsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLogsReadOnlyAccess

`CloudWatchLogsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf CloudWatch Protokolle gewährt

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchLogsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchNetworkMonitorServiceRolePolicy

`CloudWatchNetworkMonitorServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: CloudWatch Network Monitor den Zugriff auf und die Verwaltung von EC2- und VPC-Ressourcen, die Veröffentlichung von Daten CloudWatch und den Zugriff auf andere erforderliche Dienste in Ihrem Namen ermöglicht.

Diese Richtlinie verwenden

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Dezember 2023, 18:53 UTC
- Bearbeitete Zeit: 21. Dezember 2023, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchReadOnlyAccess

`CloudWatchReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf bietet CloudWatch.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchSyntheticsFullAccess

`CloudWatchSyntheticsFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf CloudWatch Synthetics bietet.

Verwenden dieser -Richtlinie

Sie können`CloudWatchSyntheticsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. November 2019, 17:39 UTC
- Bearbeitete Zeit: 6. Mai 2022, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Version der Richtlinie

Version der Richtlinie:v9 (Standard)

Die -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CloudWatchSyntheticsReadOnlyAccess

`CloudWatchSyntheticsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf CloudWatch Synthetics gewährt.

Verwenden dieser Richtlinien

Sie können`CloudWatchSyntheticsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 25. November 2019, 17:45 UTC
- Bearbeitete Zeit: 6. März 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ComprehendDataAccessRolePolicy

`ComprehendDataAccessRolePolicy`ist eine AWSverwaltete Richtlinie, die: DieAWS Servicerolle Policy for Comprehend ermöglicht den Zugriff auf S3-Ressourcen für den Datenzugriff

Verwenden dieser -Richtlinie

Sie können`ComprehendDataAccessRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. März 2019, 22:28 UTC
- Bearbeitete Zeit: 6. März 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete -verwaltete -verwaltete Version definiert die Berechtigungen für die -verwaltete -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
```

```
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ComprehendFullAccess

`ComprehendFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Comprehend bietet.

Verwenden dieser Richtlinie

Sie können`ComprehendFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2017, 18:08 UTC
- Bearbeitete Zeit: 5. Dezember 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ComprehendMedicalFullAccess

`ComprehendMedicalFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon Comprehend Medical bietet

Verwenden dieser -Richtlinie

Sie können`ComprehendMedicalFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2018, 17:55 UTC
- Bearbeitete Zeit: 27. November 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ComprehendReadOnly

`ComprehendReadOnly`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Comprehend gewährt.

Verwenden dieser -Richtlinie

Sie können`ComprehendReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2017, 18:10 UTC
- Bearbeitete Zeit: 26. April 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Version der Richtlinie

Version der Richtlinie:v11 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ComputeOptimizerReadOnlyAccess

`ComputeOptimizerReadOnlyAccess`ist einAWSverwaltete Richtliniedas: Bietet nur Lesezugriff auf ComputeOptimizer.

Verwendung dieser Richtlinie

Sie können anhängen`ComputeOptimizerReadOnlyAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie
- Zeitpunkt der Erstellung: 07. März 2020, 00:11 UTC
- Bearbeitete Zeit:28. August 2023, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie: v7(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

ComputeOptimizerServiceRolePolicy

`ComputeOptimizerServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es ComputeOptimizer ermöglicht, in Ihrem NamenAWS Dienste anzurufen und Details zur Arbeitslast zu sammeln.

Verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 3. Dezember 2019, 08:45 UTC
- Bearbeitete Zeit: 13. Juni 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalteten Richtlinien

ConfigConformsServiceRolePolicy

`ConfigConformsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Für AWSConfig die Erstellung von Konformitätspaketen erforderlich ist

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 25. Juli 2019, 21:38 UTC
- Bearbeitete Zeit: 12. Januar 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

CostOptimizationHubAdminAccess

`CostOptimizationHubAdminAccess`ist eine AWSverwaltete Richtlinie, die: Diese verwaltete Richtlinie bietet Administratorzugriff auf Cost Optimization Hub.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CostOptimizationHubAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2023, 00:03 Uhr UTC
- Bearbeitete Zeit: 19. Dezember 2023, 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CostOptimizationHubReadOnlyAccess

`CostOptimizationHubReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Diese verwaltete Richtlinie bietet schreibgeschützten Zugriff auf Cost Optimization Hub.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CostOptimizationHubReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Dezember 2023, 18:04 UTC
- Bearbeitete Zeit: 13. Dezember 2023, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CostOptimizationHubServiceRolePolicy

`CostOptimizationHubServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die es Cost Optimization Hub ermöglicht, Unternehmensinformationen abzurufen und optimierungsbezogene Daten und Metadaten zu sammeln.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2023, 08:03 UTC

- Bearbeitete Zeit: 26. November 2023, 08:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CustomerProfilesServiceLinkedRolePolicy

`CustomerProfilesServiceLinkedRolePolicy`ist eine AWSverwaltete Richtlinie, die: Amazon Connect Connect-Kundenprofilen den Zugriff aufAWS Dienste und Ressourcen in Ihrem Namen ermöglicht.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 7. März 2023, 22:56 UTC
- Bearbeitete Zeit: 7. März 2023, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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_*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

DatabaseAdministrator

`DatabaseAdministrator`ist eine AWSverwaltete Richtlinie, die: Vollzugriffsberechtigungen fürAWS Dienste und Aktionen gewährt, die zum Einrichten und Konfigurieren vonAWS Datenbankdiensten erforderlich sind.

Verwenden dieser Richtlinie

Sie können`DatabaseAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Job Funktionen
- Aufnahmezeit: 10. November 2016, 17:25 UTC
- Bearbeitete Zeit: 8. Januar 2019, 00:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

DataScientist

`DataScientist`ist eine AWSverwaltete Richtlinie, die: Berechtigungen fürAWS Datenanalysedienste gewährt.

Verwenden dieser Richtlinie

Sie können`DataScientist` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Job Funktionen
- Aufnahmezeit: 10. November 2016, 17:28 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

DAXServiceRolePolicy

`DAXServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es DAX, Netzwerkschnittstellen, Sicherheitsgruppen, Subnetze und VPCs im Namen des Kunden zu erstellen und zu verwalten

Verwenden von dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 5. März 2018, 17:51 UTC
- Bearbeitete Zeit: 5. März 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die die Berechtigungen Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON policy document

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Für die Unterstützung von Amazon CloudWatch Contributor Insights für Amazon DynamoDB sind Berechtigungen erforderlich.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen einer Gruppe oder Rollen von Benutzern, Gruppen oder Rollen einer Rolle anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 15. November 2019, 21:13 UTC
- Bearbeitete Zeit: 15. November 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

DynamoDBKinesisReplicationServiceRolePolicy

`DynamoDBKinesisReplicationServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS DynamoDB-Zugriff gewährt KinesisDataStreams

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie

- Erstellungszeit: 12. November 2020
- Bearbeitete Zeit: 12. November 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS

DynamoDBReplicationServiceRolePolicy

`DynamoDBReplicationServiceRolePolicy` ist eine -AWSverwaltete Richtlinie, die: Für DynamoDB erforderliche Berechtigungen für regionsübergreifende Datenreplikation

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 09. November 2017, 23:55 UTC
- Bearbeitungszeit: 08. Januar 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

EC2FastLaunchServiceRolePolicy

`EC2FastLaunchServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Die Richtlinie gewährt ec2fastlaunch die Vorbereitung und Verwaltung vorab bereitgestellter Snapshots im Kundenkonto und die Veröffentlichung der zugehörigen Kennzahlen.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die der Service gebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 10. Januar 2022 2022 2022 2022 2022 2022 2022 2022 2022 13:08 Januar 2022 2022 2022 2022 2022
- Bearbeitete Zeit: 10. Januar 2022, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS

Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument dokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- ErsteAWS verwaltete verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten verwalteten

EC2FleetTimeShiftableServiceRolePolicy

`EC2FleetTimeShiftableServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die EC2 Fleet Berechtigungen gewährt, Instances in future zu starten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 23. Dezember 2019, 19:47 UTC
- Bearbeitete Zeit: 23. Dezember 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie, die Berechtigungen für die Richtlinie, die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

Ec2ImageBuilderCrossAccountDistributionAccess

`Ec2ImageBuilderCrossAccountDistributionAccess`ist eine AWSverwaltete Richtlinie, die: Für eine kontoübergreifende Verteilung benötigt EC2 Image Builder Berechtigungen.

Verwenden dieser -Richtlinie

Sie können`Ec2ImageBuilderCrossAccountDistributionAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. September 2020, 19:22 UTC
- Bearbeitete Zeit: 30. September 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

EC2ImageBuilderLifecycleExecutionPolicy

`EC2ImageBuilderLifecycleExecutionPolicy`ist eine AWSverwaltete Richtlinie, die: Die ImageBuilderLifecycleExecutionPolicy EC2-Richtlinie gewährt Image Builder die Erlaubnis, Aktionen

wie das Verwerfen oder Löschen von Image Builder Builder-Image-Ressourcen und ihren zugrunde liegenden Ressourcen (AMIs, Snapshots) durchzuführen, um automatisierte Regeln für Image-Lifecycle-Management-Aufgaben zu unterstützen.

Diese Richtlinie wird verwendet

Sie können Verbindungen `EC2ImageBuilderLifecycleExecutionPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 16. November 2023, 23:23 UTC
- Bearbeitete Zeit: 16. November 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2InstanceConnect

`EC2InstanceConnect`ist eine AWSverwaltete Richtlinie, die: Es Kunden ermöglicht, EC2 Instance Connect aufzurufen, um temporäre Schlüssel für ihre EC2-Instances zu veröffentlichen und eine Verbindung über SSH oder die EC2 Instance Connect CLI herzustellen.

Verwenden dieser -Richtlinie

Sie können`EC2InstanceConnect` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. Juni 2019, 18:53 UTC
- Bearbeitete Zeit: 27. Juni 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

Ec2InstanceConnectEndpoint

`Ec2InstanceConnectEndpoint`ist eine AWSverwaltete Richtlinie, die: EC2 Instance Connect-Endpunktrichtlinie zur Verwaltung der vom Kunden erstellten EC2 Instance Connect-Endpoints

Verwenden dieser Richtlinie Richtlinie Richtlinie Richtlinie Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 24. Januar 2023, 20:19 UTC
- Bearbeitete Zeit: 24. Januar 2023, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardlinienelement Richtlinie ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument zur

```
{
  "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-*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen von Berechtigungen mit den geringsten Richtlinien und Umstellung auf Berechtigungen mit

EC2InstanceProfileForImageBuilder

`EC2InstanceProfileForImageBuilder`ist eine AWSverwaltete Richtlinie, die: EC2-Instanzprofil für den Image Builder Builder-Dienst.

Verwenden dieser Richtlinie

Sie können`EC2InstanceProfileForImageBuilder` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. Dezember 2019, 19:08 UTC
- Bearbeitete Zeit: 27. August 2020, 16:40 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der -Richtlinie definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

EC2InstanceProfileForImageBuilderECRContainerBuilds

`EC2InstanceProfileForImageBuilderECRContainerBuilds`ist eine AWSverwaltete Richtlinie, die: EC2-Instanzprofil für die Erstellung von Container-Images mit EC2 Image Builder. Diese Richtlinie gewährt dem Benutzer umfassende Berechtigungen zum Hochladen von ECR-Bildern.

Verwenden dieser Richtlinie

Sie können`EC2InstanceProfileForImageBuilderECRContainerBuilds` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 11. Dezember 2020, 19:48 UTC
- Bearbeitete Zeit: 11. Dezember 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ECRReplicationServiceRolePolicy

`ECRReplicationServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und die von ECR Replication verwendeten oder verwalteten Ressourcen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 4. Dezember 2020, 22:11 UTC
- Bearbeitete Zeit: 4. Dezember 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ElastiCacheServiceRolePolicy

`ElastiCacheServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es ElastiCache , AWS Ressourcen in Ihrem Namen zu verwalten, sofern dies für die Verwaltung Ihres Caches erforderlich ist

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten zur Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Dezember 2017, 17:50 Uhr UTC
- Bearbeitete Zeit: 28. November 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElasticLoadBalancingFullAccess

`ElasticLoadBalancingFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon und eingeschränkten Zugriff auf andere Dienste bietet ElasticLoadBalancing, die für die Bereitstellung von ElasticLoadBalancing Funktionen erforderlich sind.

Verwenden dieser Richtlinie

Sie können`ElasticLoadBalancingFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 20. September 2018, 20:42 UTC
- Bearbeitete Zeit: 29. November 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Version der Richtlinie

Version der Richtlinie:v7 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ElasticLoadBalancingReadOnly

`ElasticLoadBalancingReadOnly`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf Amazon ElasticLoadBalancing und abhängige Dienste gewährt

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElasticLoadBalancingReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. September 2018, 20:17 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsDownloadSoftwareAccess

`ElementalActivationsDownloadSoftwareAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff darauf, gekaufte Assets einzusehen und zugehörige Software und Kickstart-Dateien herunterzuladen

Verwenden dieser -Richtlinie

Sie können`ElementalActivationsDownloadSoftwareAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 8. September 2020, 17:26 UTC
- Bearbeitete Zeit: 8. September 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ElementalActivationsFullAccess

`ElementalActivationsFullAccess`ist eine AWSverwaltete Richtlinie, die: Voller Zugriff auf die gekauften Vermögenswerte von Elemental Appliances und Software sowie deren Bearbeitung

Verwenden dieser Richtlinie

Sie können`ElementalActivationsFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 4. Juni 2020, 21:00 UTC
- Bearbeitete Zeit: 4. Juni 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ElementalActivationsGenerateLicenses

`ElementalActivationsGenerateLicenses`ist eine AWSverwaltete Richtlinie, die: Zugriff auf gekaufte Ressourcen und Generierung von Softwarelizenzen für ausstehende Aktivierungen

Verwenden dieser Richtlinien

Sie können`ElementalActivationsGenerateLicenses` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. August 2020, 18:28 UTC
- Bearbeitete Zeit: 28. August 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte und Umstellung auf Berechtigungen mitAWS den geringsten Richtlinien

ElementalActivationsReadOnlyAccess

`ElementalActivationsReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Schreibgeschützter Zugriff auf die detaillierte Liste der gekauften Assets, die demAWS-Konto des Benutzers zugeordnet sind

Verwenden dieser Richtlinien

Sie können`ElementalActivationsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 28. August 2020, 16:51 UTC
- Bearbeitete Zeit: 28. August 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Dokument mit Richtlinien

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ElementalAppliancesSoftwareFullAccess

`ElementalAppliancesSoftwareFullAccess`ist eine AWSverwaltete Richtlinie, die: Voller Zugriff auf Angebote und Bestellungen von Elemental Appliances and Software sowie deren Bearbeitung

Verwenden dieser -Richtlinie

Sie können`ElementalAppliancesSoftwareFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 31. Juli 2019, 16:28 UTC
- Bearbeitete Zeit: 5. Februar 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

ElementalAppliancesSoftwareReadOnlyAccess

`ElementalAppliancesSoftwareReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Angebote und Bestellungen von Elemental Appliances and Software nur Lesezugriff

Verwenden dieser -Richtlinie

Sie können`ElementalAppliancesSoftwareReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 1. April 2020, 22:31 UTC
- Bearbeitete Zeit: 1. April 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ElementalSupportCenterFullAccess

`ElementalSupportCenterFullAccess`ist eine AWSverwaltete Richtlinie, die: Voller Zugriff auf Supportfälle und Inhalte des Produktsupports von Elemental Appliance und Software sowie die Möglichkeit, entsprechende Maßnahmen zu ergreifen

Verwenden dieser -Richtlinie

Sie können`ElementalSupportCenterFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. November 2020, 18:08 UTC
- Bearbeitete Zeit: 5. Februar 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie definiert die Berechtigungen für die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

EMRDescribeClusterPolicyForEMRWAL

`EMRDescribeClusterPolicyForEMRWAL`List eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Leserechte, die es dem WAL-Service für Amazon EMR ermöglichen, den Status eines Clusters zu finden und zurückzugeben

Verwendung dieser Richtlinie

Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen auszuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für dienstverknüpfte Rollen
- Aufnahmezeit: 15. Juni 2023, 23:30 UTC
- Bearbeitete Zeit: 15. Juni 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

FMSServiceRolePolicy

`FMSServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Zugriffsrichtlinie, die es einer mit dem FM-Dienst verknüpften Rolle ermöglicht, FM-bezogene Aktionen für von FM verwaltete Ressourcen innerhalb eines Unternehmenskontos des KundenAWS auszuführen.

Von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 28. März 2018, 23:01 UTC
- Bearbeitete Zeit: 21. April 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v28 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinien

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
```

```
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
```

```
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
```

```
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "ram",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
```

```
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:PutResourcePolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und die geringsten Berechtigungen und die geringsten Berechtigungen für die geringsten Berechtigungen

FSxDeleteServiceLinkedRoleAccess

`FSxDeleteServiceLinkedRoleAccess`ist eine AWSverwaltete Richtlinie, die: Amazon FSx das Löschen seiner Service Linked Roles für den Zugriff auf Amazon S3 ermöglicht

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 28. November 2018, 10:40 UTC
- Bearbeitete Zeit: 28. November 2018, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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_*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- VerwendenAWS verwalteter Richtlinien

GameLiftGameServerGroupPolicy

`GameLiftGameServerGroupPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die es Gamelift ermöglicht, Kundenressourcen GameServerGroups zu verwalten

Verwenden dieser -Richtlinie

Sie können`GameLiftGameServerGroupPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 3. April 2020, 23:12 UTC
- Bearbeitete Zeit: 13. Mai 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

GlobalAcceleratorFullAccess

`GlobalAcceleratorFullAccess`ist eine AWSverwaltete Richtlinie, die: GlobalAccelerator Benutzern vollen Zugriff auf alle APIs gewährt

Verwenden dieser -Richtlinie

Sie können`GlobalAcceleratorFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2018, 02:44 UTC
- Bearbeitete Zeit: 4. Dezember 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

GlobalAcceleratorReadOnlyAccess

`GlobalAcceleratorReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: GlobalAccelerator Benutzern den Zugriff auf schreibgeschützten APIs ermöglicht

Verwenden dieser -Richtlinie

Sie können`GlobalAcceleratorReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2018, 02:41 UTC
- Bearbeitete Zeit: 27. November 2018, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

GreengrassOTAUpdateArtifactAccess

`GreengrassOTAUpdateArtifactAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf die Greengrass OTA Update-Artefakte in allen Greengrass-Regionen bietet

Verwenden dieser Richtlinie

Sie können`GreengrassOTAUpdateArtifactAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 29. November 2017, 18:11 UTC
- Bearbeitete Zeit: 18. Dezember 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

GroundTruthSyntheticConsoleFullAccess

`GroundTruthSyntheticConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen, die für die Nutzung aller Funktionen der SageMaker Ground Truth Synthetic Console erforderlich sind.

Verwenden dieser -Richtlinie

Sie können`GroundTruthSyntheticConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. August 2022, 15:58 UTC
- Bearbeitete Zeit: 25. August 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

GroundTruthSyntheticConsoleReadOnlyAccess

`GroundTruthSyntheticConsoleReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt nur Lesezugriff auf SageMaker Ground Truth Synthetic über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie könnenGroundTruthSyntheticConsoleReadOnlyAccess an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 25. August 2022, 15:58 UTC
- Bearbeitete Zeit: 25. August 2022, 15:58 UTC
- ARN: arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

Health_OrganizationsServiceRolePolicy

`Health_OrganizationsServiceRolePolicy` ist eine -AWSverwaltete Richtlinie, die: AWS Zustandsrichtlinie zur Aktivierung der Funktion Organisationsansicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 16. Dezember 2019, 13:28 UTC
- Bearbeitungszeit: 06. Februar 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

IAMAccessAdvisorReadOnly

`IAMAccessAdvisorReadOnly`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Zugriff auf das Lesen aller vom IAM Access Advisor bereitgestellten Zugriffsinformationen, z. B. Informationen, auf die der Dienst zuletzt zugegriffen hat.

Verwenden dieser -Richtlinie

Sie können`IAMAccessAdvisorReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie

- Aufnahmezeit: 21. Juni 2019, 19:33 UTC
- Bearbeitete Zeit: 21. Juni 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Berechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

IAMAccessAnalyzerFullAccess

`IAMAccessAnalyzerFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf IAM Access Analyzer bietet

Verwenden dieser Richtlinie

Sie können`IAMAccessAnalyzerFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 2. Dezember 2019, 17:12 UTC
- Bearbeitete Zeit: 2. Dezember 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

IAMAccessAnalyzerReadOnlyAccess

`IAMAccessAnalyzerReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf IAM Access Analyzer-Ressourcen gewährt

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMAccessAnalyzerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Dezember 2019, 17:12 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMFullAccess

`IAMFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf IAM über die bietetAWS Management Console.

Verwenden dieser Richtlinie

Sie können`IAMFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 21. Juni 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der Richtlinie definiert die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

IAMReadOnlyAccess

`IAMReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Ermöglicht nur Lesezugriff auf IAM über dieAWS Management Console.

Verwenden dieser -Richtlinie

Sie können`IAMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 25. Januar 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -verwaltete -verwaltete Version ist die -verwaltete Version, die die Berechtigungen für die -verwaltete -verwaltete -verwaltete -verwaltete Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf den geringsten Berechtigungen

IAMSelfManageServiceSpecificCredentials

`IAMSelfManageServiceSpecificCredentials`ist eine AWSverwaltete Richtlinie, die: Es einem IAM-Benutzer ermöglicht, seine eigenen dienstspezifischen Anmeldeinformationen zu verwalten.

Verwenden dieser Richtlinien

Sie können`IAMSelfManageServiceSpecificCredentials` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. Dezember 2016, 17:25 UTC

- Bearbeitete Zeit: 22. Dezember 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

IAMUserChangePassword

`IAMUserChangePassword`ist eine AWSverwaltete Richtlinie, die: Es einem IAM-Benutzer ermöglicht, sein eigenes Passwort zu ändern.

Verwenden dieser -Richtlinie

Sie können`IAMUserChangePassword` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 15. November 2016, 00:25 UTC
- Bearbeitete Zeit: 15. November 2016, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

IAMUserSSHKeys

`IAMUserSSHKeys`ist eine AWSverwaltete Richtlinie, die: IAM-Benutzern die Möglichkeit bietet, ihre eigenen SSH-Schlüssel zu verwalten.

Verwenden dieser -Richtlinie

Sie können`IAMUserSSHKeys` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Juli 2015, 17:08 UTC
- Bearbeitete Zeit: 9. Juli 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

IVSFullAccess

`IVSFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf den Interactive Video Service (IVS) bietet. Dazu gehören auch Berechtigungen für abhängige Dienste, die für den vollständigen Zugriff auf die IVS-Konsole erforderlich sind.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IVSFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Dezember 2023, 21:20 UTC
- Bearbeitete Zeit: 13. Dezember 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IVSReadOnlyAccess

`IVSReadOnlyAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf IVS-Streaming-APIs mit niedriger Latenz und Echtzeit-Streaming-APIs

Verwenden dieser Richtlinie

Sie können `IVSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 05. Dezember 2023, 18:00 UTC
- Bearbeitungszeit: 16. Februar 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

IVSRecordToS3

`IVSRecordToS3`ist eine AWSverwaltete Richtlinie, die: Service Linked Role zur Ausführung von S3 PutObject zur Aufzeichnung von IVS-Live-Streams

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 5. Dezember 2020, 00:10 UTC
- Bearbeitete Zeit: 5. Dezember 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtdokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

KafkaConnectServiceRolePolicy

`KafkaConnectServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie erteilt Kafka Connect die Erlaubnis,AWS Ressourcen in Ihrem Namen zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 7. September 2021, 13:12 UTC
- Bearbeitete Zeit: 7. September 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

KafkaServiceRolePolicy

`KafkaServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: IAM Service Linked Role Policy für Kafka.

Verwenden von IAM-Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die servicegebundene Rolle ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 15. November 2018, 23:31 UTC
- Bearbeitete Zeit: 28. April 2023, 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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_*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien

KeyspacesReplicationServiceRolePolicy

`KeyspacesReplicationServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Für Keyspaces erforderliche Berechtigungen für die regionsübergreifende Datenreplikation

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 2. Mai 2023, 16:15 UTC
- Bearbeitete Zeit: 2. Mai 2023, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

LakeFormationDataAccessServiceRolePolicy

`LakeFormationDataAccessServiceRolePolicy` ist eine -AWS verwaltete Richtlinie, die: Richtlinie zum Gewähren des temporären Datenzugriffs auf Lake-Formation-Ressourcen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 20. Juni 2019, 20:46 UTC
- Bearbeitungszeit: 06. Februar 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

LexBotPolicy

`LexBotPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie für denAWS Lex-Bot-Anwendungsfall

Verwenden diese Richtlinie Verwenden dieser Richtlinie verwenden

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie

- Aufnahmezeit: 17. Februar 2017, 22:18 UTC
- Bearbeitete Zeit: 13. November 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

J-Richtlinienelement

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinienelement Richtlinienelement Richtlinienelement Richtlinienelement Richtlinienelement Richtlinienelement Richtlinienelement Richtlinienelement Richtlinie

LexChannelPolicy

`LexChannelPolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie für denAWS Lex Channel-Anwendungsfall

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. Februar 2017, 23:23 UTC
- Bearbeitete Zeit: 17. Februar 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-JSON-Dokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

LightsailExportAccess

`LightsailExportAccess`ist eine AWSverwaltete Richtlinie, die:AWS Lightsail Service Linked Role Policy, die Berechtigungen für den Export von Ressourcen gewährt

von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 28. September 2018, 16:35 UTC
- Bearbeitete Zeit: 15. Januar 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtdokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung verwalteter Richtlinien

MediaConnectGatewayInstanceRolePolicy

`MediaConnectGatewayInstanceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt die Erlaubnis, MediaConnect Gateway-Instances auf einem MediaConnect Gateway zu registrieren.

Verwenden dieser Richtlinie

Sie können`MediaConnectGatewayInstanceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 22. März 2023, 20:43 UTC
- Bearbeitete Zeit: 22. März 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
```

```
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

MediaPackageServiceRolePolicy

`MediaPackageServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Erlaubt das MediaPackage Veröffentlichen von Protokollen unter CloudWatch

Verwenden von IAM-Richtlinien

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. September 2020, 17:45 UTC
- Bearbeitete Zeit: 18. September 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

MemoryDBServiceRolePolicy

`MemoryDBServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie ermöglicht es MemoryDB,AWS -Ressourcen in Ihrem Namen nach Bedarf für die Verwaltung Ihrer -Ressourcen zu verwalten.

Verwenden dieser Richtlinie

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen angehängt werden.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 17. August 2021, 22:34 UTC
- Bearbeitete Zeit: 18. August 2021, 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

MigrationHubDMSAccessServiceRolePolicy

`MigrationHubDMSAccessServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, nach der der Database Migration Service die Rolle im Kundenkonto übernimmt und Migration Hub anruft

Verwenden dieser Richtlinie Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. Juni 2019, 17:50 UTC
- Bearbeitete Zeit: 7. Oktober 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die StandardRichtlinie ist die Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-RichtRichtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

MigrationHubServiceRolePolicy

`MigrationHubServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Es Migration Hub ermöglicht, Application Discovery Service in Ihrem Namen aufzurufen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die servicegebundene Rolle zugeordnet, die serviceDurchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. Juni 2019, 17:22 UTC
- Bearbeitete Zeit: 06. August 2020, 18:08 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v3 (Standard)

Die Standardversion der Richtlinie ist die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

MigrationHubSMSAccessServiceRolePolicy

`MigrationHubSMSAccessServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie, nach der der Server Migration Service die Rolle im Kundenkonto übernimmt und Migration Hub aufruft

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. Juni 2019, 18:30 UTC
- Bearbeitete Zeit: 7. Oktober 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

MonitronServiceRolePolicy

`MonitronServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Richtlinie für die dienstverknüpfteAWS Monitron-Rolle, die den Zugriff auf die erforderlichen Kundenressourcen gewährt.

Verwenden von von von von Richtlinien

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 2. Mai 2022, 19:22 UTC
- Bearbeitete Zeit: 2. Mai 2022, 19:22 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSONSONSONSONSONSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS verwalteter Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

NeptuneConsoleFullAccess

`NeptuneConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf die Verwaltung von Amazon Neptune mithilfe der bietet. AWS Management Console Beachten Sie, dass diese

Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos, Berechtigungen zum Erstellen und Bearbeiten von Amazon EC2 EC2-Instances und VPC-Konfigurationen, Berechtigungen zum Anzeigen und Auflisten von Schlüsseln in Amazon KMS sowie vollen Zugriff auf Amazon RDS gewährt. Weitere Informationen finden Sie unter https://aws.amazon.com/neptune/faqs/.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `NeptuneConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juni 2018, 21:35 UTC
- Bearbeitete Zeit: 30. November 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneFullAccess

`NeptuneFullAccess` ist eine von AWS verwaltete Richtlinie, die: Bietet vollen Zugriff auf Amazon Neptune . Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf die Veröffentlichung aller SNS-Themen innerhalb des Kontos und vollen Zugriff auf Amazon RDS gewährt. Weitere Informationen finden Sie unter https://aws.amazon.com/neptune/faqs/..

Verwenden dieser Richtlinie

Sie können `NeptuneFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2018, 19:17 UTC
- Bearbeitungszeit: 22. Januar 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Richtlinienversion

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

NeptuneGraphReadOnlyAccess

`NeptuneGraphReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur-Lese-Zugriff auf alle Amazon Neptune Analytics-Ressourcen sowie Nur-Lese-Berechtigungen für abhängige Services bietet.

Diese Richtlinie wird verwendet

Sie können Verbindungen `NeptuneGraphReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2023, 07:32 UTC
- Bearbeitete Zeit: 30. November 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneReadOnlyAccess

`NeptuneReadOnlyAccess` ist eine -AWSverwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf Amazon Neptune . Beachten Sie, dass diese Richtlinie auch Zugriff auf Amazon-RDS-Ressourcen gewährt. Weitere Informationen finden Sie unter https://aws.amazon.com/neptune/faqs/..

Verwenden dieser Richtlinie

Sie können `NeptuneReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie

- Erstellungszeit: 30. Mai 2018, 19:16 UTC
- Bearbeitungszeit: 22. Januar 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

NetworkAdministrator

`NetworkAdministrator`ist eine AWSverwaltete Richtlinie, die: Vollzugriffsberechtigungen fürAWS Dienste und Aktionen gewährt, die für die Einrichtung und Konfiguration vonAWS Netzwerkressourcen erforderlich sind.

Verwenden dieser Richtlinie

Sie können`NetworkAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Job Funktionen
- Aufnahmezeit: 10. November 2016, 17:31 UTC
- Bearbeitete Zeit: 16. September 2021, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Version der Richtlinie

Version der Richtlinie:v11 (Standard)

Die -Standardversion der -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

OAMFullAccess

`OAMFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf CloudWatch Observability Access Manager bietet

Verwenden von dieser -Richtlinie

Sie können`OAMFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2022, 13:38 UTC
- Bearbeitete Zeit: 27. November 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

OAMReadOnlyAccess

`OAMReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Read Only Zugriff auf CloudWatch Observability Access Manager bietet

Verwenden dieser Richtlinien

Sie können`OAMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2022, 13:29 UTC
- Bearbeitete Zeit: 27. November 2022, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

PartnerCentralAccountManagementUserRoleAssociation

`PartnerCentralAccountManagementUserRoleAssociation`ist eine AWSverwaltete Richtlinie, die: Zugriff auf das Zuordnen und Trennen von Partnern Central-Benutzern zu IAM-Rollen ermöglicht

Diese Richtlinie wird verwendet

Sie können Verbindungen `PartnerCentralAccountManagementUserRoleAssociation` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2023, 02:03 UTC

- Bearbeitete Zeit: 10. November 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

PowerUserAccess

`PowerUserAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf AWS Dienste und Ressourcen bietet, aber keine Verwaltung von Benutzern und Gruppen zulässt.

Verwendung dieser Richtlinie

Sie können Verbindungen `PowerUserAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 06. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 06. Juli 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`ist eine AWSverwaltete Richtlinie, die: Richtlinie, die vom QuickSight Team für den Zugriff auf Kundendaten verwendet wird, die von S3 Storage Management Analytics erstellt wurden.

Verwenden dieser -Richtlinie

Sie können`QuickSightAccessForS3StorageManagementAnalyticsReadOnly` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 12. Juni 2017, 18:18 UTC
- Bearbeitete Zeit: 8. Oktober 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -verwaltete -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwalRichtlinien und Umstellung auf Berechtigungen

RDSCloudHsmAuthorizationRole

`RDSCloudHsmAuthorizationRole`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Amazon RDS-Servicerolle.

Verwenden dieser -Richtlinie

Sie können`RDSCloudHsmAuthorizationRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 26. September 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ReadOnlyAccess

`ReadOnlyAccess` ist eine -AWS verwaltete Richtlinie, die: Bietet schreibgeschützten Zugriff auf - AWS Services und -Ressourcen.

Verwenden dieser Richtlinie

Sie können `ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 06. Februar 2015, 18:39 UTC
- Bearbeitungszeit: 05. Februar 2024, 15:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Richtlinienversion

Richtlinienversion: v111 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine - AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
```

```
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",
        "access-analyzer:ListAccessPreviews",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "aoss:BatchGetCollection",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListSecurityConfigs",
```

```
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorEntity",
        "appflow:DescribeConnectorFields",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeConnectors",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DescribeFlows",
        "appflow:ListConnectorEntities",
        "appflow:ListConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "application-autoscaling:ListTagsForResource",
        "applicationinsights:Describe*",
```

```
        "applicationinsights:List*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:Get*",
        "appsync:List*",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeWorkspace",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:QueryMetrics",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
```

```
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
```

```
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
```

```
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "budgets:Describe*",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCostAllocationTags",
```

```
        "ce:ListCostCategoryDefinitions",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams",
        "chatbot:ListMicrosoftTeamsUserIdentities",
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
```

```
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListRepositoriesInDomain",
        "codeartifact:ListTagsForResource",
        "codeartifact:ReadFromRepository",
        "codebuild:BatchGet*",
        "codebuild:DescribeCodeCoverages",
        "codebuild:DescribeTestCases",
        "codebuild:List*",
```

```
        "codecatalyst:GetBillingAuthorization",
        "codecatalyst:GetConnection",
        "codecatalyst:GetPendingConnection",
        "codecatalyst:ListConnections",
        "codecatalyst:ListIamRolesForConnection",
        "codecatalyst:ListTagsForResource",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:List*",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetRepositorySyncStatus",
        "codestar-connections:GetResourceSyncStatus",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListRepositorySyncDefinitions",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar-notifications:ListTargets",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "cognito-identity:Describe*",
```

```
        "cognito-identity:GetCredentialsForIdentity",
        "cognito-identity:GetIdentityPoolAnalytics",
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
        "cognito-idp:Get*",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
```

```
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:GetTrafficDistribution",
        "connect:List*",
        "consoleapp:GetDeviceIdentity",
        "consoleapp:ListDeviceIdentities",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:Get*",
        "dataexchange:List*",
```

```
        "datapipeline:Describe*",
        "datapipeline:EvaluateExpression",
        "datapipeline:Get*",
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
        "datasync:List*",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
```

```
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "ec2:Describe*",
        "ec2:Get*",
```

```
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elastic-inference:DescribeAcceleratorOfferings",
        "elastic-inference:DescribeAccelerators",
        "elastic-inference:DescribeAcceleratorTypes",
        "elastic-inference:ListTagsForResource",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
```

```
        "elastictranscoder:Read*",
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:Get*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
```

```
        "fis:GetTargetAccountConfiguration",
        "fis:GetTargetResourceType",
        "fis:ListActions",
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperiments",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
        "fms:GetProtocolsList",
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
        "fms:ListMemberAccounts",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
```

```
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
        "frauddetector:GetDeleteEventsByEventTypeStatus",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
        "freertos:List*",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
```

```
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTriggers",
        "glue:BatchGetWorkflows",
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalogImportStatus",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMapping",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
```

```
        "glue:GetSchemaVersionsDiff",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:GetWorkflowRunProperties",
        "glue:GetWorkflowRuns",
        "glue:ListCrawlers",
        "glue:ListCrawls",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "glue:QuerySchemaVersionMetadata",
        "glue:SearchTables",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListPermissions",
        "grafana:ListTagsForResource",
        "grafana:ListVersions",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:Get*",
        "greengrass:List*",
        "groundstation:DescribeContact",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
```

```
        "groundstation:ListConfigs",
        "groundstation:ListContacts",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
```

```
        "importexport:Get*",
        "importexport:List*",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iotanalytics:Describe*",
```

```
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotroborunner:GetDestination",
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
```

```
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListWorkers",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
```

```
        "iotwireless:ListQueuedMessages",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:Describe*",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
```

```
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSources",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListEntityPersonas",
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
```

```
        "lakeformation:GetResourceLfTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
        "launchwizard:GetIpAddress",
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
```

```
        "lex:Get*",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
```

```
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAnomalies",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
```

```
        "lookoutequipment:DescribeDataIngestionJob",
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:DescribeLabel",
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModels",
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListApplicationVersions",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
```

```
        "m2:ListDataSetImportHistory",
        "m2:ListDataSets",
        "m2:ListDeployments",
        "m2:ListEngineVersions",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetFindingStatistics",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
```

```
        "macie2:ListTagsForResource",
        "macie2:SearchResources",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "medialive:DescribeChannel",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:ListChannels",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListTagsForResource",
```

```
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
```

```
        "mobileanalytics:Get*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnections",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
```

```
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetEula",
        "nimble:GetFeatureMap",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileMember",
        "nimble:GetStreamingImage",
        "nimble:GetStreamingSession",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:GetStudioMember",
        "nimble:ListEulaAcceptances",
        "nimble:ListEulas",
        "nimble:ListLaunchProfileMembers",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStreamingSessions",
        "nimble:ListStudioComponents",
        "nimble:ListStudioMembers",
        "nimble:ListStudios",
        "nimble:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "oam:GetLink",
```

```
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "omics:Get*",
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
```

```
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "personalize:Describe*",
        "personalize:Get*",
        "personalize:List*",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "polly:Describe*",
        "polly:Get*",
        "polly:List*",
        "polly:SynthesizeSpeech",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetPriceListFileUrl",
        "pricing:GetProducts",
        "pricing:ListPriceLists",
        "proton:GetDeployment",
        "proton:GetEnvironment",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:ListDeployments",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceInstances",
        "proton:ListServices",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
```

```
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ViewPurchaseOrders",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
```

```
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
```

```
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "sagemaker-groundtruth-synthetic:GetAccountDetails",
```

```
        "sagemaker-groundtruth-synthetic:GetBatch",
        "sagemaker-groundtruth-synthetic:GetProject",
        "sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
        "sagemaker-groundtruth-synthetic:ListBatchSummaries",
        "sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
        "sagemaker-groundtruth-synthetic:ListProjectSummaries",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
```

```
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
        "signer:ListTagsForResource",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
```

```
        "snowball:Get*",
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "storagegateway:Describe*",
        "storagegateway:List*",
```

```
            "sts:GetAccessKeyInfo",
            "sts:GetCallerIdentity",
            "sts:GetSessionToken",
            "support:DescribeAttachment",
            "support:DescribeCases",
            "support:DescribeCommunications",
            "support:DescribeServices",
            "support:DescribeSeverityLevels",
            "support:DescribeTrustedAdvisorCheckRefreshStatuses",
            "support:DescribeTrustedAdvisorCheckResult",
            "support:DescribeTrustedAdvisorChecks",
            "support:DescribeTrustedAdvisorCheckSummaries",
            "supportplans:GetSupportPlan",
            "supportplans:GetSupportPlanUpdateStatus",
            "sustainability:GetCarbonFootprintSummary",
            "swf:Count*",
            "swf:Describe*",
            "swf:Get*",
            "swf:List*",
            "synthetics:Describe*",
            "synthetics:Get*",
            "synthetics:List*",
            "tag:DescribeReportCreation",
            "tag:Get*",
            "tax:GetExemptions",
            "tax:GetTaxInheritance",
            "tax:GetTaxInterview",
            "tax:GetTaxRegistration",
            "tax:GetTaxRegistrationDocument",
            "tax:ListTaxRegistrations",
            "timestream:DescribeBatchLoadTask",
            "timestream:DescribeDatabase",
            "timestream:DescribeEndpoints",
            "timestream:DescribeTable",
            "timestream:ListBatchLoadTasks",
            "timestream:ListDatabases",
            "timestream:ListMeasures",
            "timestream:ListTables",
            "timestream:ListTagsForResource",
            "tnb:GetSolFunctionInstance",
            "tnb:GetSolFunctionPackage",
            "tnb:GetSolFunctionPackageContent",
            "tnb:GetSolFunctionPackageDescriptor",
            "tnb:GetSolNetworkInstance",
```

```
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
```

```
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:ListAnswers",
        "wellarchitected:ListCheckDetails",
        "wellarchitected:ListCheckSummaries",
        "wellarchitected:ListLenses",
        "wellarchitected:ListLensReviewImprovements",
        "wellarchitected:ListLensReviews",
        "wellarchitected:ListLensShares",
        "wellarchitected:ListMilestones",
        "wellarchitected:ListNotifications",
        "wellarchitected:ListProfileNotifications",
        "wellarchitected:ListProfiles",
        "wellarchitected:ListProfileShares",
        "wellarchitected:ListReviewTemplateAnswers",
```

```
        "wellarchitected:ListReviewTemplates",
        "wellarchitected:ListShareInvitations",
        "wellarchitected:ListTagsForResource",
        "wellarchitected:ListTemplateShares",
        "wellarchitected:ListWorkloads",
        "wellarchitected:ListWorkloadShares",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

ResourceGroupsandTagEditorFullAccess

`ResourceGroupsandTagEditorFullAccess`ist einAWSverwaltete Richtliniedas: Bietet vollen Zugriff auf Ressourcengruppen und den Tag-Editor.

Verwenden Sie diese Richtlinie

Sie können anhängen`ResourceGroupsandTagEditorFullAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie
- Zeitpunkt der Erstellung: 06. Februar 2015, 18:39 Uhr UTC
- Bearbeitete Zeit:10. August 2023, 13:29 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Version der Richtlinie

Version der Richtlinie: v6(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

ResourceGroupsandTagEditorReadOnlyAccess

`ResourceGroupsandTagEditorReadOnlyAccess`ist einAWSverwaltete RichtlinieDas: Ermöglicht den Zugriff auf Ressourcengruppen und den Tag-Editor, erlaubt jedoch nicht die Bearbeitung von Tags über den Tag-Editor.

Diese Richtlinie wird verwendet

Sie können anhängen`ResourceGroupsandTagEditorReadOnlyAccess`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ:AWSverwaltete Richtlinie

- Zeitpunkt der Erstellung: 06. Februar 2015, 18:39 UTC
- Bearbeitete Zeit:10. August 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie: v3(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

ResourceGroupsServiceRolePolicy

`ResourceGroupsServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die:AWS Resource Groups erlaubt, dieAWS Dienste abzufragen, denen Ihre Ressourcen gehören, um die Gruppe zu behalten up-to-date

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 5. Januar 2023, 16:57 UTC
- Bearbeitete Zeit: 5. Januar 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

ROSAAmazonEBSCSIDriverOperatorPolicy

`ROSAAmazonEBSCSIDriverOperatorPolicy`ist eine AWSverwaltete Richtlinie, die: Es demOpenShift Amazon EBS Container Storage Interface (CSI) -Treiberoperator ermöglicht, den Amazon EBS CSI-Treiber auf einem Red HatOpenShift Service onAWS (ROSA) -Cluster zu installieren und zu verwalten. Amazon EBS CSI-Treiber ermöglicht ROSA-Cluster die Verwaltung des Lebenszyklus von Amazon-EBS-Volumes für persistente Volumes.

Verwenden dieser Richtlinie

Sie können`ROSAAmazonEBSCSIDriverOperatorPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 20. April 2023, 22:36 UTC
- Bearbeitete Zeit: 20. April 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-JSON-Richtlinien

```
{
  "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"
          ]
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien mit -verwaltete Richtlinien Richtlinien mit den geringBerechtigungen Berechtigungen mit den geringBerechtigungen Berechtigungen

ROSACloudNetworkConfigOperatorPolicy

`ROSACloudNetworkConfigOperatorPolicy`ist eine AWSverwaltete Richtlinie, die: Es demOpenShift Cloud Network Config Controller Operator ermöglicht, Netzwerkressourcen für die Verwendung durch das Red HatOpenShift Service onAWS (ROSA) Cluster-Netzwerk-Overlay bereitzustellen und zu verwalten. DerOpenShift Cloud Network Operator stellt im Namen der Netzwerk-Plugins eine Schnittstelle zuAWS APIs her überCustomResourceDefinitions. Der Betreiber verwendet diese Richtlinienberechtigungen, um private IP-Adressen für Amazon EC2 EC2-Instances als Teil des ROSA-Clusters zu verwalten.

Verwenden von dieser -Richtlinie mit der

Sie können`ROSACloudNetworkConfigOperatorPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 20. April 2023, 22:34 UTC
- Bearbeitete Zeit: 20. April 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt, wird die Standardversion der RichtlinieAWS überprüft, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinie von JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von IAM-Richtlinie zum Hinzufügen von IAM-Richtlinie und -AM-Richtlinie
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete -Richtlinie und Umstellung auf Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen mit den geringsten Berechtigungen

ROSAControlPlaneOperatorPolicy

`ROSAControlPlaneOperatorPolicy`ist eine AWSverwaltete Richtlinie, die: Es Red Hat OpenShift Service auf der AWS (ROSA) -Steuerungsebene ermöglicht, die Ressourcen des ROSA-Clusters, Amazon EC2 und Amazon Route 53 zu verwalten.

Verwendung dieser Richtlinie

Sie können Verbindungen `ROSAControlPlaneOperatorPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Diensträgerrollen
- Aufnahmezeit: 24. April 2023, 23:02 UTC
- Bearbeitete Zeit: 30. Juni 2023, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

ROSAImageRegistryOperatorPolicy

`ROSAImageRegistryOperatorPolicy`ist eine AWSverwaltete Richtlinie, die: dem OpenShift Image Registry Operator die Bereitstellung und Verwaltung von Amazon S3 S3-Buckets und Objekten für die Nutzung durch die Cluster-Image-Registry Red Hat OpenShift Service on AWS (ROSA) ermöglicht, um die ROSA-Speicheranforderungen zu erfüllen. Der OpenShift Image Registry Operator installiert und verwaltet die interne Registrierung eines Red Hat OpenShift Clusters.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `ROSAImageRegistryOperatorPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. April 2023, 20:13 UTC
- Bearbeitete Zeit: 12. Dezember 2023, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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}/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAIngressOperatorPolicy

`ROSAIngressOperatorPolicy`ist eine AWSverwaltete Richtlinie, die: Es demOpenShift Ingress Operator ermöglicht, Loadbalancer und Domain Name System (DNS) -Konfigurationen für Red HatOpenShift Service onAWS (ROSA) -Cluster bereitzustellen und zu verwalten. Die Richtlinie ermöglicht den Lesezugriff auf Tag-Werte, die der Betreiber nach Route 53 53-Ressourcen filtert, um gehostete Zonen zu erkennen.

Verwenden von von von dieser -Richtlinie

Sie können`ROSAIngressOperatorPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 20. April 2023, 22:37 UTC
- Bearbeitete Zeit: 20. April 2023, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der -Richtlinie ist die -Standardversion der -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

Dokument mit den JSON-Richtlinie

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen von von IAM-Identitätsberechtigungen und -verwaltete Richtlinien von -
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien und Umstellung auf verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

ROSAInstallerPolicy

`ROSAInstallerPolicy` ist eine von AWS verwaltete Richtlinie, die: Ermöglicht dem Installationsprogramm von Red Hat OpenShift Service in AWS (ROSA), AWS Ressourcen zu verwalten, die die Installation von ROSA-Clustern unterstützen. Dazu gehört die Verwaltung von Instance-Profilen für ROSA-Worker-Knoten.

Verwenden dieser Richtlinie

Sie können `ROSAInstallerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 06. Juni 2023, 21:00 Uhr UTC
- Bearbeitungszeit: 26. Januar 2024, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

ROSAKMSProviderPolicy

`ROSAKMSProviderPolicy`ist eine AWSverwaltete Richtlinie, die: Es dem integrierten ROSAAWS Encryption Provider ermöglicht,AWS Key Management Service (KMS) -Schlüssel zu verwalten, um die etCD-Datenverschlüsselung mithilfe eines vom Kunden bereitgestelltenAWS KMS-Schlüssels zu unterstützen. Die Richtlinie ermöglicht die Verschlüsselung und Entschlüsselung von Daten mithilfe von KMS-Schlüsseln.

Verwenden von -Richtlinie

Sie können`ROSAKMSProviderPolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 27. April 2023, 20:10 UTC
- Bearbeitete Zeit: 27. April 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
```

```
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinien
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten sten sten sten sten sten sten sten sten sten sten sten sten

ROSAKubeControllerPolicy

`ROSAKubeControllerPolicy`ist eine AWSverwaltete Richtlinie, die: dem ROSA Kubernetes-Controller ermöglicht, Amazon EC2-, Elastic Load Balancing- (ELB) - und AWS Key Management Service (KMS) -Ressourcen für einen ROSA-Cluster zu verwalten.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAKubeControllerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. April 2023, 20:09 UTC
- Bearbeitete Zeit: 16. Oktober 2023, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAManageSubscription

`ROSAManageSubscription`ist einAWSverwaltete Richtliniedas: Diese Richtlinie bietet die Berechtigungen, die für die Verwaltung von Red Hat erforderlich sindOpenShiftService amAWS(ROSA) -Abonnement.

Verwendung dieser Richtlinie

Sie können anhängen`ROSAManageSubscription`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten der Richtlinie

- Typ:AWSverwaltete Richtlinie
- Zeit der Erstellung: 11. April 2022, 20:58 Uhr UTC
- Uhrzeit der Bearbeitung:04. August 2023, 19:59 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Version der Richtlinie

Version der Richtlinie: v2(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eineAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

ROSANodePoolManagementPolicy

`ROSANodePoolManagementPolicy`ist eine AWSverwaltete Richtlinie, die: Red Hat OpenShift Service on AWS (ROSA) die Verwaltung von Cluster-EC2-Instances als Worker-Knoten ermöglicht, einschließlich der Berechtigung, Sicherheitsgruppen zu konfigurieren und Instances und Volumes zu kennzeichnen. Diese Richtlinie ermöglicht auch die Verwendung von EC2-Instances mit Festplattenverschlüsselung, die durch AWS Key Management Service (KMS) -Schlüssel bereitgestellt wird.

Verwenden dieser -Richtlinie

Sie können Verbindungen `ROSANodePoolManagementPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Dienstrollen
- Erstellungszeit: 8. Juni 2023, 20:48 UTC
- Bearbeitete Zeit: 08. Juni 2023, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ROSASRESupportPolicy

`ROSASRESupportPolicy` ist eine -AWSverwaltete Richtlinie, die: Stellt ROSA Site Reliability Engineering (SRE) die Berechtigungen bereit, die erforderlich sind, um zunächst AWS Ressourcen zu beobachten, zu diagnostizieren und zu unterstützen, die mit Red Hat OpenShift Service in AWS (ROSA)-Clustern verknüpft sind, einschließlich der Möglichkeit, den Zustand des ROSA-Clusterknotens zu ändern.

Verwenden dieser Richtlinie

Sie können `ROSASRESupportPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : Servicerollenrichtlinie
- Erstellungszeit: 01. Juni 2023, 14:36 UTC
- Bearbeitungszeit: 22. Januar 2024, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWSRessource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
```

```
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "VPCNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudtrail",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "DescribeLoadBalancers",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeStaleSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAddressesAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeAddressesAttribute",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
    },
    {
      "Sid" : "DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ManageInstanceLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

ROSAWorkerInstancePolicy

`ROSAWorkerInstancePolicy`ist eine AWSverwaltete Richtlinie, die: Red HatOpenShift Service onAWS (ROSA) -Worker-Knoten in Ihrem Konto den schreibgeschützten Zugriff auf Amazon EC2 EC2-Instances undAWS-Regionen für das Compute Node-Lifecycle-Management ermöglicht.

Verwenden dieser -Richtlinie

Sie können`ROSAWorkerInstancePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 20. April 2023, 22:35 UTC
- Bearbeitete Zeit: 20. April 2023, 22:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-JSON-Richtlinie

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Richtlinie
- Versionierung für IAM-Richtlinien verstehen

- Erste Schritte mitAWS -verwalverwalund Umstellung auf Berechtigungen

Route53RecoveryReadinessServiceRolePolicy

`Route53RecoveryReadinessServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Service Linked Role Policy for Route 53 Recovery Readiness

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 15. Juli 2021, 16:06 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v5 (Standard)

Die Standardversion ist die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

J-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS Berechtigungen und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

Route53ResolverServiceRolePolicy

`Route53ResolverServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und die von Route53 Resolver verwendeten oder verwalteten Ressourcen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügt.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 12. August 2020, 17:47 UTC
- Bearbeitete Zeit: 12. August 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

S3StorageLensServiceRolePolicy

`S3StorageLensServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und die von S3 Storage Lens verwendeten oder verwalteten Ressourcen ermöglicht

Verwenden dieser

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 18. November 2020, 18:15 UTC
- Bearbeitete Zeit: 18. November 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardversion der Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete

SecretsManagerReadWrite

`SecretsManagerReadWrite` ist eine von AWS verwaltete Richtlinie, die: Bietet Lese-/Schreibzugriff auf AWS Secrets Manager über die AWS Management Console. Hinweis: Dies schließt IAM-Aktionen aus. Kombinieren Sie daher mit IAM, FullAccess wenn eine Rotationskonfiguration erforderlich ist.

Verwenden dieser Richtlinie

Sie können `SecretsManagerReadWrite` an Ihre Benutzer, Gruppen und Rollen anfügen.

Richtliniendetails

- Typ : AWS verwaltete Richtlinie
- Erstellungszeit: 04. April 2018, 18:05 UTC
- Bearbeitungszeit: 22. Februar 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Richtlinienversion

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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-*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen eines Berechtigungssatzes mithilfe AWS von verwalteten Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS von verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

SecurityAudit

`SecurityAudit`ist eine AWSverwaltete Richtlinie, die: Die Vorlage für die Sicherheitsüberprüfung gewährt Zugriff auf lesbare Metadaten zur Sicherheitskonfiguration. Es ist nützlich für Software, die die Konfiguration eines überprüftAWS-Konto.

Verwenden Sie diese Richtlinie

Sie können Verbindungen `SecurityAudit` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 14. Dezember 2023, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Version der Richtlinie

Richtlinienversion: v41 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "BaseSecurityAuditStatement",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
```

```
        "account:GetAlternateContact",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApiCache",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListControls",
```

```
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeRegionSettings",
        "backup:GetBackupVaultAccessPolicy",
        "backup:ListBackupVaults",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:ListTagsForResource",
        "cloudwatch:ListDashboards",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:ListProjects",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
```

```
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListInstances",
        "dataexchange:ListDataSets",
```

```
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayAttachmentPropagations",
```

```
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListUpdates",
        "elastic-inference:DescribeAccelerators",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
```

```
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeVault",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
        "glue:GetJobs",
        "glue:GetResourcePolicy",
```

```
        "glue:GetSecurityConfigurations",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedEntities",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEvents",
        "health:DescribeEventTypes",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
```

```
        "iotevents:ListInputs",
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:List*",
        "lex:DescribeBot",
```

```
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancers",
        "logs:Describe*",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "machinelearning:DescribeMLModels",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:ListContainers",
        "memorydb:DescribeClusters",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
```

```
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
        "opsworks:DescribeStacks",
        "organizations:Describe*",
        "organizations:List*",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
```

```
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
```

```
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
        "ses:GetAccountSendingEnabled",
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:ListAssociations",
        "ssm:ListAssociationVersions",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "ssm:ListInventoryEntries",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeAccountAssignmentCreationStatus",
```

```
        "sso:DescribePermissionSet",
        "sso:DescribePermissionsPolicies",
        "sso:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "storagegateway:DescribeBandwidthRateLimit",
        "storagegateway:DescribeCache",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:DescribeMaintenanceStartTime",
        "storagegateway:DescribeNFSFileShares",
        "storagegateway:DescribeSnapshotSchedule",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:DescribeTapeArchives",
        "storagegateway:DescribeTapeRecoveryPoints",
        "storagegateway:DescribeTapes",
        "storagegateway:DescribeUploadBuffer",
        "storagegateway:DescribeVTLDevices",
        "storagegateway:DescribeWorkingStorage",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
```

```
        "transcribe:ListMedicalTranscriptionJobs",
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLforResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ]
    },
    {
      "Effect" : "Allow",
      "Sid" : "APIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
```

```
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecurityLakeServiceLinkedRole

`SecurityLakeServiceLinkedRole` ist eine -AWS verwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen zum Betreiben des Amazon-Security-Lake-Service in Ihrem Namen

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es dem Service ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Richtliniendetails

- Typ : Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 29. November 2022, 14:03 UTC
- Bearbeitungszeit: 29. Februar 2024, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Richtlinienversion

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eine -

AWS Ressource stellt, AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versioning für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

ServerMigration_ServiceRole

`ServerMigration_ServiceRole`ist eine AWSverwaltete Richtlinie, die: Berechtigungen, die es demAWS Server Migration Service ermöglichen, VMs zu EC2 zu migrieren: es dem Server Migration Service ermöglicht, die migrierten Ressourcen im EC2-Konto des Kunden zu platzieren.

Verwenden dieser -Richtlinie

Sie können`ServerMigration_ServiceRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 11. August 2020, 20:41 UTC
- Bearbeitete Zeit: 15. Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*/*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

ServerMigrationConnector

`ServerMigrationConnector`ist eine AWSverwaltete Richtlinie, die: Berechtigungen, die es demAWS Server Migration Connector ermöglichen, virtuelle Maschinen zu EC2 zu migrieren. Ermöglicht die Kommunikation mit demAWS Server Migration Service, Lese-/Schreibzugriff auf S3-Buckets, die mit 'sms-b-' und 'import-to-ec2' beginnen, sowie auf die Buckets, die für dasAWS Server Migration Connector-Upgrade, die Registrierung desAWS Server Migration Connectors mitAWS und das Hochladen von Metriken verwendet werdenAWS.

Verwenden dieser Richtlinie

Sie können`ServerMigrationConnector` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Oktober 2016, 21:45 UTC
- Bearbeitete Zeit: 24. Oktober 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardversion ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ServerMigrationServiceConsoleFullAccess

`ServerMigrationServiceConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Erforderliche Berechtigungen für die Nutzung aller Funktionen der Server Migration Service Console

Verwenden dieser -Richtlinie

Sie können`ServerMigrationServiceConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 9. Mai 2020, 17:18 UTC
- Bearbeitete Zeit: 20. Juli 2020, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

ServerMigrationServiceLaunchRole

`ServerMigrationServiceLaunchRole`ist eine AWSverwaltete Richtlinie, die: Berechtigungen, die es demAWS Server Migration Service ermöglichen, relevanteAWS RessourcenAWS-Konto für den Kunden zu erstellen und zu aktualisieren, um migrierte Server und Anwendungen zu starten.

Verwenden dieser -Richtlinie

Sie können`ServerMigrationServiceLaunchRole` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 26. November 2018, 19:53 UTC
- Bearbeitete Zeit: 15. Oktober 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Standardversion ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource

stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

ServerMigrationServiceRoleForInstanceValidation

`ServerMigrationServiceRoleForInstanceValidation`ist eine AWSverwaltete Richtlinie, die: Berechtigungen, um derAWS SMS zu erlauben, das verwendete Datenvalidierungsskript auszuführen und das erfolgreiche oder fehlgeschlagene Skript an die SMS zurückzusenden

Verwenden dieser Richtlinie

Sie können`ServerMigrationServiceRoleForInstanceValidation` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstorollenrichtlinie
- Aufnahmezeit: 20. Juli 2020, 22:25 UTC
- Bearbeitete Zeit: 20. Juli 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Standardrichtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen

ServiceQuotasFullAccess

`ServiceQuotasFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Service Quotas bietet

Verwenden

Sie können`ServiceQuotasFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2019, 15:44 UTC
- Bearbeitete Zeit: 4. Februar 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Version der Richtlinie

Version der Richtlinie:v4 (Standard)

Die -Richtlinie definiert die Berechtigungen Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

ServiceQuotasReadOnlyAccess

`ServiceQuotasReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Nur Lesezugriff auf Service Quotas gewährt

Verwenden dieser Richtlinien

Sie können`ServiceQuotasReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 24. Juni 2019, 15:31 UTC
- Bearbeitete Zeit: 21. Dezember 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Richtlinienversion definiert die Berechtigungen für die -Richtlinie. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- ErsteAWS Schritte mit den geringsten Berechtigungen

ServiceQuotasServiceRolePolicy

`ServiceQuotasServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Service Quotas die Erstellung von Supportfällen in Ihrem Namen ermöglicht

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen angehängt.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Erstellungszeit: 22. Mai 2019, 20:44 UTC
- Bearbeitete Zeit: 24. Juni 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

SimpleWorkflowFullAccess

`SimpleWorkflowFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf den Simple Workflow-Konfigurationsdienst bietet.

Verwenden dieser -Richtlinie

Sie können`SimpleWorkflowFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

SupportUser

`SupportUser`ist einAWSverwaltete Richtliniedass: Diese Richtlinie gewährt Berechtigungen zur Behebung und Lösung von Problemen in einemAWS-Konto. Diese Richtlinie ermöglicht es dem Benutzer auch, Kontakt aufzunehmenAWSUnterstützung bei der Erstellung und Verwaltung von Fällen.

Diese Richtlinie verwenden

Sie können anhängen`SupportUser`an Ihre Benutzer, Gruppen und Rollen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für berufliche Funktionen
- Zeit der Erstellung: 10. November 2016, 17:21 Uhr UTC
- Bearbeitete Zeit:25. August 2023, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Version der Richtlinie

Version der Richtlinie: v8(Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf stelltAWSRessource,AWSüberprüft die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zugelassen werden soll.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mitAWSverwaltete Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Fangen Sie an mitAWSverwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten

SystemAdministrator

`SystemAdministrator`ist eine AWSverwaltete Richtlinie, die: volle Zugriffsberechtigungen gewährt, die für Ressourcen erforderlich sind, die für Anwendungs- und Entwicklungsvorgänge erforderlich sind.

Verwenden dieser -Richtlinie

Sie können`SystemAdministrator` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Job Funktionen
- Aufnahmezeit: 10. November 2016, 17:23 UTC
- Bearbeitete Zeit: 24. August 2020, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Version der Richtlinie

Version der Richtlinie:v6 (Standard)

Die -Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

TranslateFullAccess

`TranslateFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf Amazon Translate bietet.

Verwenden dieser -Richtlinie

Sie können`TranslateFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 27. November 2018, 23:36 UTC
- Bearbeitete Zeit: 8. Januar 2020, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die -Standardversion der -Richtlinie ist die -Version, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

TranslateReadOnly

`TranslateReadOnly`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon Translate gewährt.

Verwenden Sie diese -Richtlinie

Sie können Verbindungen `TranslateReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2017, 18:22 UTC
- Bearbeitete Zeit: 24. Mai 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtlinie

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mit AWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

ViewOnlyAccess

`ViewOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie gewährt Berechtigungen zum Anzeigen von Ressourcen und grundlegenden Metadaten für alleAWS Dienste.

Verwenden dieser -Richtlinie

Sie können`ViewOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Richtlinie für Job Funktionen
- Aufnahmezeit: 10. November 2016, 17:20 UTC
- Bearbeitete Zeit: 06. März 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v17 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "batch:ListJobs",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudhsm:ListAvailableZones",
        "cloudhsm:ListHapgs",
        "cloudhsm:ListHsms",
        "cloudhsm:ListLunaClients",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dms:List*",
        "ds:DescribeDirectories",
```

```
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHost*",
        "ec2:DescribeIdFormat",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
        "ec2:DescribePlacementGroups",
```

```
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnGateways",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elastic-inference:DescribeAccelerators",
        "elastic-inference:DescribeAcceleratorTypes",
        "elastic-inference:DescribeAcceleratorOfferings",
        "elastic-inference:ListTagsForResource",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fsx:DescribeFileSystems",
```

```
        "gamelift:List*",
        "glacier:List*",
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kms:ListKeys",
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBots",
        "lex:GetIntentVersions",
        "lex:GetIntents",
        "lex:GetSlotTypeVersions",
        "lex:GetSlotTypes",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
        "opsworks-cm:Describe*",
```

```
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
        "ses:List*",
        "shield:List*",
        "sns:List*",
        "sqs:ListQueues",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListGateways",
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "trustedadvisor:Describe*",
```

```
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

VMImportExportRoleForAWSConnector

`VMImportExportRoleForAWSConnector`ist eine AWSverwaltete Richtlinie, die: Standardrichtlinie für die Servicerolle VM Import/Export für Kunden, die denAWS Connector verwenden. Der VM Import/Export-Dienst übernimmt im Rahmen dieser Richtlinie eine Rolle bei der Erfüllung von Migrationsanforderungen für virtuelle Maschinen von der virtuellenAWS Connector-Appliance. (Beachten Sie, dass derAWS Connector die verwaltete RichtlinieAWSConnector "" verwendet, um im Namen des Kunden Anfragen an den VM Import/Export-Service zu stellen.) Bietet die Möglichkeit, AMIs und EBS-Snapshots zu erstellen, EBS-Snapshot-Attribute zu ändern, „Describe*“ -Aufrufe fürimport-to-ec EC2-Objekte zu tätigen und aus S3-Buckets zu lesen, die mit '2' beginnen.

Verwenden dieser -Richtlinie

Sie können`VMImportExportRoleForAWSConnector` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Servicerollenrichtlinie
- Aufnahmezeit: 3. September 2015, 20:48 UTC
- Bearbeitete Zeit: 3. September 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt, wird die Standardversion der RichtlinieAWS überprüft, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

VPCLatticeFullAccess

`VPCLatticeFullAccess`ist eine AWSverwaltete Richtlinie, die: vollen Zugriff auf Amazon VPC Lattice und Zugriff auf Abhängigkeitsdienste bietet.

Verwenden dieser Richtlinien

Sie können`VPCLatticeFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. März 2023, 02:49 UTC
- Bearbeitete Zeit: 30. März 2023, 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS

Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

VPCLatticeReadOnlyAccess

`VPCLatticeReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf Amazon VPC Lattice über denAWS Management Console und eingeschränkten Zugriff auf Abhängigkeitsdienste bietet.

Verwenden dieser -Richtlinie

Sie können`VPCLatticeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. März 2023, 02:47 UTC
- Bearbeitete Zeit: 30. März 2023, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

VPCLatticeServicesInvokeAccess

`VPCLatticeServicesInvokeAccess`ist eine AWSverwaltete Richtlinie, die: Zugriff auf das Aufrufen von Amazon VPC Lattice-Diensten bietet.

Verwenden dieser Richtlinien

Sie können`VPCLatticeServicesInvokeAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 30. März 2023, 02:45 UTC
- Bearbeitete Zeit: 30. März 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Richtlinie ist die -Richtlinie, die die Berechtigungen für die -Funktion definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

WAFLoggingServiceRolePolicy

`WAFLoggingServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Spiegelreflexkamera erstellen, um Kundenprotokolle in einen Firehose-Stream zu schreiben

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie zu Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 24. August 2018, 21:05 UTC
- Bearbeitete Zeit: 24. August 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standardlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinienlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

WAFRegionalLoggingServiceRolePolicy

`WAFRegionalLoggingServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Spiegelreflexkamera erstellen, um Kundenprotokolle in einen Firehose-Stream zu schreiben

Verwenden von dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie an Ihre Benutzer, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 24. August 2018, 18:40 UTC

- Bearbeitete Zeit: 24. August 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die Standard-Version ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtlinienelement

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien

WAFV2LoggingServiceRolePolicy

`WAFV2LoggingServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: Diese Richtlinie erstellt eine serviceverknüpfte Rolle, die es derAWS WAF ermöglicht, Protokolle an Amazon Kinesis Data Firehose zu schreiben.

Verwenden dieser Richtlinie

Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die die Durchführung von Aktionen in Ihrem Namen ermöglicht. Sie können diese Richtlinie Ihren Benutzern, Gruppen oder Rollen anfügen.

Einzelheiten der Richtlinie

- Typ: Serviceverknüpfte Rollenrichtlinie
- Aufnahmezeit: 7. November 2019, 00:40 UTC
- Bearbeitete Zeit: 23. Juli 2020, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

WellArchitectedConsoleFullAccess

`WellArchitectedConsoleFullAccess`ist eine AWSverwaltete Richtlinie, die: Vollzugriff auf dasAWS Well-Architected Tool bietet über dieAWS Management Console

Verwenden dieser -Richtlinie

Sie können`WellArchitectedConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2018, 18:19 UTC
- Bearbeitete Zeit: 29. November 2018, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -verwaltete -verwaltete Version definiert die Berechtigungen für die -Funktion. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen

WellArchitectedConsoleReadOnlyAccess

`WellArchitectedConsoleReadOnlyAccess`ist eine AWSverwaltete Richtlinie, die: Lesezugriff auf AWS Well-Architected Tool über die AWS Management Console

Verwendung dieser Richtlinie

Sie können Verbindungen `WellArchitectedConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten der Richtlinie

- Typ: AWS verwaltete Richtlinie
- Aufnahmezeit: 29. November 2018, 18:21 UTC
- Bearbeitete Zeit: 29. Juni 2023, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage für den Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien in IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen

- Beginnen Sie mit AWS verwalteten Richtlinien und gehen Sie zu Berechtigungen mit den geringsten Rechten über

WorkLinkServiceRolePolicy

`WorkLinkServiceRolePolicy`ist eine AWSverwaltete Richtlinie, die: den Zugriff aufAWS-Services und von Amazon verwendete oder verwaltete Ressourcen ermöglicht WorkLink

Verwenden dieser -Richtlinie

Sie können`WorkLinkServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anhängen.

Einzelheiten der Richtlinie

- Typ:AWS verwaltete Richtlinie
- Aufnahmezeit: 23. Januar 2019, 19:03 UTC
- Bearbeitete Zeit: 23. Januar 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Version der Richtlinie

Version der Richtlinie:v1 (Standard)

Die -Standardversion der -Richtlinie ist die -Standardversion, die die Berechtigungen für die -Standard-Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anforderung für den Zugriff auf eineAWS Ressource stellt,AWS überprüft die Standardversion der Richtlinie, um festzustellen, ob die Anforderung zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfeAWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Versionierung für IAM-Richtlinien verstehen
- Erste Schritte mitAWS -verwaltete Richtlinien und Umstellung auf -verwaltete Richtlinien

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.