



# **Google Cloud-Berechtigungen und erforderliche Firewall-Regeln**

NetApp Console setup and administration

NetApp  
February 11, 2026

# Inhalt

- Google Cloud-Berechtigungen und erforderliche Firewall-Regeln . . . . . 1
  - Google Cloud-Berechtigungen für den Konsolenagenten . . . . . 1
    - Berechtigungen für Google Cloud-Nutzerkonten . . . . . 1
    - Dienstkontoberechtigungen . . . . . 3
    - So werden Google Cloud-Berechtigungen verwendet . . . . . 8
    - Änderungsprotokoll . . . . . 19
  - Agent-Firewallregeln in Google Cloud . . . . . 22
    - Eingehende Regeln . . . . . 22
    - Ausgangsregeln . . . . . 22

# Google Cloud-Berechtigungen und erforderliche Firewall-Regeln

## Google Cloud-Berechtigungen für den Konsolenagenten

Der Konsolenagent benötigt Berechtigungen zum Ausführen von Aktionen in Google Cloud. Diese Berechtigungen sind in einer benutzerdefinierten Rolle enthalten, die von NetApp bereitgestellt wird. Sie sollten verstehen, was der Agent mit diesen Berechtigungen macht.

### Berechtigungen für Google Cloud-Nutzerkonten

Die unten stehende benutzerdefinierte Rolle gewährt einem Google Cloud-Benutzer die erforderlichen Berechtigungen zum Bereitstellen eines Agenten. Weisen Sie diese benutzerdefinierte Rolle dem Benutzer zu, der den Agenten bereitstellen wird.

## Google Cloud-Nutzerkontoberechtigungen anzeigen

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

- `config.operations.get`
- `config.deployments.delete`
- `config.deployments.deleteState`
- `config.deployments.get`
- `config.deployments.getState`
- `config.deployments.list`
- `config.deployments.update`
- `config.deployments.updateState`
- `config.previews.get`
- `config.previews.list`
- `config.revisions.get`
- `config.resources.list`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `resourcemanager.projects.get`
- `compute.instances.setServiceAccount`
- `iam.serviceAccounts.actAs`
- `iam.serviceAccounts.create`
- `iam.serviceAccounts.list`
- `iam.serviceAccountKeys.create`
- `storage.buckets.create`
- `storage.buckets.get`
- `storage.objects.create`
- `storage.folders.create`
- `storage.objects.list`

## Dienstkontoberechtigungen

Die unten stehende benutzerdefinierte Rolle weist dem mit dem Console-Agenten verknüpften Google Cloud-Dienstkonto die Berechtigungen zu, die zum Verwalten von Ressourcen und Prozessen in Ihrem Google Cloud-Netzwerk erforderlich sind.

Weisen Sie diese benutzerdefinierte Rolle einem Dienstkonto zu, das mit der Console-Agent-VM verbunden ist.

- ["Google Cloud-Berechtigungen für den Standardmodus einrichten"](#)
- ["Berechtigungen für den eingeschränkten Modus einrichten"](#)

## Google-Dienstkontoberechtigungen anzeigen

Stellen Sie sicher, dass die Rolle auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt oder entfernt werden. Im Änderungsprotokoll sind alle erforderlichen neuen Berechtigungen aufgeführt. [Überprüfen Sie das Änderungsprotokoll der Google-Berechtigungen.](#) [Lesen Sie, wie Sie Google Cloud-Dienstkonten hinzufügen.](#)

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent.
stage: GA
includedPermissions:
- cloudbuild.builds.get
- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
- config.artifacts.import
- config.deployments.create
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getLock
- config.deployments.getState
- config.deployments.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.deployments.getLock
- config.deployments.list
- config.deployments.lock
- config.operations.get
- config.previews.get
- config.previews.list
- config.resources.list
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionBackendServices.update
- compute.networks.updatePolicy
```

- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.list
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.backendServices.create
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.forwardingRules.update
- compute.globalOperations.get
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop



- compute.instances.updateDisplayDevice
- compute.instances.use
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.get
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.instances.setMinCpuPlatform
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.regionBackendServices.delete
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list

- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- logging.logEntries.create
- logging.logEntries.route
- monitoring.timeSeries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.list
- storage.objects.update
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.get
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.objects.get
- storage.objects.list
- storage.buckets.getIamPolicy

## So werden Google Cloud-Berechtigungen verwendet

Der Console-Agent nutzt die Berechtigungen in der benutzerdefinierten Rolle, um Cloud Volumes ONTAP Ressourcen und NetApp -Datendienstprozesse in Ihrem Google Cloud-Netzwerk zu verwalten. In den folgenden Abschnitten wird beschrieben, wie der Agent diese Berechtigungen nutzt.

### Für Cloud Volumes ONTAP verwendete Berechtigungen

Der Console-Agent nutzt die Berechtigungen in der benutzerdefinierten Rolle, um Cloud Volumes ONTAP Ressourcen und -Prozesse in Ihrem Google Cloud-Netzwerk zu verwalten. In den folgenden Abschnitten wird beschrieben, wie der Agent diese Berechtigungen nutzt.

## Berechtigungen für Cloud Volumes ONTAP

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
config.deployments.create	Um die virtuelle Maschineninstanz Cloud Volumes ONTAP mithilfe von Google Cloud Infrastructure Manager bereitzustellen.	Ja	Nein	Nein
config.deployments.delete		Nein	Nein	Ja
config.deployments.deleteState		Nein	Nein	Ja
config.deployments.get		Nein	Ja	Nein
config.deployments.getLock		Nein	Ja	Nein
config.deployments.getState		Nein	Ja	Nein
config.deployments.list		Nein	Ja	Nein
config.deployments.lock		Nein	Ja	Nein
config.deployments.update		Nein	Ja	Nein
config.deployments.updateState		Nein	Ja	Nein
config.operations.get		Nein	Ja	Nein
config.preview.get		Nein	Ja	Nein
config.preview.list		Nein	Ja	Nein
config.resources.list		Nein	Ja	Nein
config.revisions.get		Nein	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.disks.create	Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP.	Ja	Ja	Nein
compute.disks.createSnapshot		Nein	Ja	Nein
compute.disks.delete		Nein	Ja	Ja
compute.disks.get		Nein	Ja	Nein
compute.disks.list		Ja	Ja	Nein
compute.disks.setLabels		Ja	Ja	Nein
compute.disks.use		Nein	Ja	Nein
compute.firewalls.create	So erstellen Sie Firewall-Regeln für Cloud Volumes ONTAP.	Ja	Nein	Nein
compute.firewalls.delete		Nein	Ja	Ja
compute.firewalls.get		Ja	Ja	Nein
compute.firewalls.list		Ja	Ja	Nein
compute.forwardingRules.create	Erstellen Sie Weiterleitungsregeln für das Routing des Datenverkehrs zu Backend-Diensten.	Nein	Ja	Nein
compute.forwardingRules.delete	Vorhandene Weiterleitungsregeln löschen.	Nein	Ja	Nein
compute.forwardingRules.get	Details zu bestehenden Weiterleitungsregeln abrufen.	Nein	Ja	Nein
compute.forwardingRules.setLabels	Labels für Weiterleitungsregeln der Organisation festlegen oder aktualisieren.	Nein	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.forwardingRules.update	Aktualisieren Sie bestehende Weiterleitungsregeln für das Verkehrsmanagement.	Nein	Ja	Nein
compute.globalOperations.get	Um den Status von Vorgängen abzurufen.	Ja	Ja	Nein
compute.healthChecks.create	Erstellung und Verwaltung von Gesundheitsprüfungen zur Überwachung des Zustands der Backend-Dienste.	Nein	Ja	Nein
compute.healthChecks.delete		Nein	Ja	Nein
compute.healthChecks.get		Nein	Ja	Nein
compute.healthChecks.useReadOnly		Nein	Ja	Nein
compute.images.get	Um Bilder für VM-Instanzen zu erhalten.	Ja	Nein	Nein
compute.images.getFromFamily		Ja	Nein	Nein
compute.images.list		Ja	Nein	Nein
compute.images.useReadOnly		Ja	Nein	Nein
compute.instances.attachDisk	So schließen Sie Festplatten an Cloud Volumes ONTAP an und trennen sie davon.	Ja	Ja	Nein
compute.instances.detachDisk		Nein	Ja	Ja
compute.instances.create	Zum Erstellen und Löschen von Cloud Volumes ONTAP VM-Instanzen.	Ja	Nein	Nein
compute.instances.delete		Nein	Nein	Ja
compute.instances.get	Zum Auflisten von VM-Instanzen.	Ja	Ja	Nein
compute.instances.getSerialPortOutput	Um Konsolenprotokolle zu erhalten.	Ja	Ja	Nein
compute.instances.list	Zum Abrufen der Liste der Instanzen in einer Zone.	Ja	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.instances.setDeletionProtection	Um den Löschschutz für die Instanz festzulegen.	Ja	Nein	Nein
compute.instances.setLabels	Um Beschriftungen hinzuzufügen.	Ja	Nein	Nein
compute.instances.setMachineType	So ändern Sie den Maschinentyp für Cloud Volumes ONTAP.	Ja	Ja	Nein
compute.instances.setMinCpuPlatform		Ja	Ja	Nein
compute.instances.setMetadata	Um Metadaten hinzuzufügen.	Ja	Ja	Nein
compute.instances.setTags	So fügen Sie Tags für Firewall-Regeln hinzu.	Ja	Ja	Nein
compute.instances.start	So starten und stoppen Sie Cloud Volumes ONTAP.	Ja	Ja	Nein
compute.instances.stop		Ja	Ja	Nein
compute.instances.updateDisplayDevice		Ja	Ja	Nein
compute.instances.use	Nutzen Sie virtuelle Maschineninstanzen (Start-, Stopp- und Verbindungsvorgänge).	Nein	Ja	Nein
compute.machineTypes.get	Um die Anzahl der Kerne zu ermitteln und die Quoten zu überprüfen.	Ja	Nein	Nein
compute.projects.get	Zur Unterstützung mehrerer Projekte.	Ja	Nein	Nein
compute.resourcePolicies.create	Ressourcenrichtlinien für die automatisierte Ressourcenverwaltung erstellen und verwalten.	Nein	Ja	Nein
compute.resourcePolicies.delete		Nein	Ja	Nein
compute.resourcePolicies.get		Nein	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.snapshots.create	Zum Erstellen und Verwalten persistenter Festplatten-Snapshots.	Ja	Ja	Nein
compute.snapshots.delete		Nein	Ja	Ja
compute.snapshots.get		Nein	Ja	Nein
compute.snapshots.list		Nein	Ja	Nein
compute.snapshots.setLabels		Ja	Ja	Nein
compute.networks.get	Um die Netzwerkinformationen zu erhalten, die zum Erstellen einer neuen Cloud Volumes ONTAP VM-Instanz erforderlich sind.	Ja	Ja	Nein
compute.networks.list		Ja	Ja	Nein
compute.regions.get		Ja	Ja	Nein
compute.regions.list		Ja	Ja	Nein
compute.subnetworks.get		Ja	Ja	Nein
compute.subnetworks.list		Ja	Ja	Nein
compute.zoneOperations.get		Ja	Ja	Nein
compute.zones.get		Ja	Ja	Nein
compute.zones.list		Ja	Ja	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
deploymentmanager.compositeTypes.get	So stellen Sie die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereit.	Ja	Nein	Nein
deploymentmanager.compositeTypes.list		Ja	Nein	Nein
deploymentmanager.deployments.create		Ja	Nein	Nein
deploymentmanager.deployments.delete		Ja	Nein	Nein
deploymentmanager.deployments.get		Ja	Nein	Nein
deploymentmanager.deployments.list		Ja	Nein	Nein
deploymentmanager.manifests.get		Ja	Nein	Nein
deploymentmanager.manifests.list		Ja	Nein	Nein
deploymentmanager.operations.get		Ja	Nein	Nein
deploymentmanager.operations.list		Ja	Nein	Nein
deploymentmanager.resources.get		Ja	Nein	Nein
deploymentmanager.resources.list		Ja	Nein	Nein
deploymentmanager.typeProviders.get		Ja	Nein	Nein
deploymentmanager.typeProviders.list		Ja	Nein	Nein
deploymentmanager.types.get		Ja	Nein	Nein
deploymentmanager.types.list		Ja	Nein	Nein
logging.logEntries.list	Um Stack-Log-Laufwerke zu erhalten.	Ja	Ja	Nein
logging.privateLogEntries.list		Ja	Ja	Nein



Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
logging.logEntries.create	Protokolleinträge erstellen und weiterleiten für Überwachung, Fehlersuche und Prüfung.	Ja	Ja	Nein
logging.logEntries.route		Ja	Ja	Nein
resourceManager.projects.get	Zur Unterstützung mehrerer Projekte.	Ja	Ja	Nein
storage.buckets.create	So erstellen und verwalten Sie einen Google Cloud Storage-Bucket für die Datenschichtung.	Ja	Ja	Nein
storage.buckets.delete		Nein	Ja	Ja
storage.buckets.get		Nein	Ja	Nein
storage.buckets.list		Nein	Ja	Nein
storage.buckets.update		Nein	Ja	Nein
cloudkms.cryptoKeyVersions.useToEncrypt	So verwenden Sie vom Kunden verwaltete Verschlüsselungsschlüssel vom Cloud Key Management Service mit Cloud Volumes ONTAP.	Ja	Ja	Nein
cloudkms.cryptoKeys.get		Ja	Ja	Nein
cloudkms.cryptoKeys.list		Ja	Ja	Nein
cloudkms.keyRings.list		Ja	Ja	Nein
cloudbuild.builds.get		Ja	Nein	Nein
compute.instances.setServiceAccount	So richten Sie ein Dienstkonto auf der Cloud Volumes ONTAP -Instanz ein. Dieses Dienstkonto bietet Berechtigungen für die Datenschichtung in einem Google Cloud Storage-Bucket.	Ja	Ja	Nein
iam.serviceAccounts.actAs		Ja	Nein	Nein
iam.serviceAccounts.create		Ja	Nein	Nein
iam.serviceAccounts.getIamPolicy		Ja	Ja	Nein
iam.serviceAccounts.list		Ja	Ja	Nein
iam.serviceAccounts.keys.create		Ja	Nein	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
storage.objects.create	Objekte (Dateien) im Google Cloud Storage-Bucket erstellen und verwalten.	Ja	Ja	Nein
storage.objects.delete		Nein	Nein	Ja
storage.objects.get		Ja	Ja	Nein
storage.objects.list		Ja	Ja	Nein
compute.addresses.list	Zum Abrufen der Adressen in einer Region beim Bereitstellen eines HA-Paares.	Ja	Nein	Nein
compute.addresses.createInternal	Erstellen Sie interne IP-Adressen innerhalb des VPC-Netzwerks zur Ressourcenzuweisung.	Nein	Ja	Nein
compute.addresses.deleteInternal	Interne IP-Adressen zur Ressourcenbereinigung löschen.	Nein	Ja	Nein
compute.addresses.setLabels	Aktualisieren Sie die Bezeichnungen der Adressressource.	Nein	Ja	Nein
compute.addresses.useInternal	Für die Netzwerkkommunikation interne IP-Adressen verwenden.	Nein	Ja	Nein
compute.backendServices.create	So konfigurieren Sie einen Backend-Dienst zum Verteilen des Datenverkehrs in einem HA-Paar.	Ja	Nein	Nein

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
compute.regionBackendServices.create	Backend-Dienste für das Traffic-Routing erstellen und verwalten.	Ja	Nein	Nein
compute.regionBackendServices.delete		Nein	Ja	Nein
compute.regionBackendServices.get		Ja	Nein	Nein
compute.regionBackendServices.update		Ja	Ja	Nein
compute.regionBackendServices.list		Ja	Nein	Nein
compute.regionBackendServices.use		Nein	Ja	Nein
compute.networks.updatePolicy	So wenden Sie Firewall-Regeln auf die VPCs und Subnetze für ein HA-Paar an.	Ja	Nein	Nein
compute.instanceGroups.get	Zum Erstellen und Verwalten von Speicher-VMs auf Cloud Volumes ONTAP HA-Paaren.	Ja	Ja	Nein
compute.addresses.get		Ja	Ja	Nein
compute.instances.updateNetworkInterface		Ja	Ja	Nein
compute.instanceGroups.create		Nein	Ja	Nein
compute.instanceGroups.delete		Nein	Ja	Nein
compute.instanceGroups.update		Nein	Ja	Nein
compute.instanceGroups.use		Nein	Ja	Nein
monitoring.timeSerieslist	Um Informationen zu Google Cloud Storage-Buckets zu erhalten.	Ja	Ja	Nein
storage.buckets.getIamPolicy		Ja	Ja	Nein

## Für NetApp Backup and Recovery verwendete Berechtigungen

Der Console-Agent nutzt die Berechtigungen in der benutzerdefinierten Rolle, um NetApp Backup and Recovery Ressourcen und -Prozesse in Ihrem Google Cloud-Netzwerk zu verwalten. In den folgenden Abschnitten wird beschrieben, wie der Agent diese Berechtigungen nutzt.

### Berechtigungen für NetApp Backup and Recovery anzeigen

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
<ul style="list-style-type: none"><li>• <code>cloudkms.cryptoKeys.get</code></li><li>• <code>cloudkms.cryptoKeys.getIamPolicy</code></li><li>• <code>cloudkms.cryptoKeys.list</code></li><li>• <code>cloudkms.cryptoKeys.setIamPolicy</code></li><li>• <code>cloudkms.keyRings.get</code></li><li>• <code>cloudkms.keyRings.getIamPolicy</code></li><li>• <code>cloudkms.keyRings.list</code></li><li>• <code>cloudkms.keyRings.setIamPolicy</code></li></ul>	So wählen Sie im Aktivierungsassistenten von NetApp Backup and Recovery Ihre eigenen, vom Kunden verwalteten Schlüssel aus, anstatt die standardmäßigen, von Google verwalteten Verschlüsselungsschlüssel zu verwenden.	Ja	Ja	Nein

## Für die NetApp Data Classification verwendete Berechtigungen

Der Console-Agent nutzt die Berechtigungen in der benutzerdefinierten Rolle, um NetApp Data Classification Ressourcen und -Prozesse in Ihrem Google Cloud-Netzwerk zu verwalten. In den folgenden Abschnitten wird beschrieben, wie der Agent diese Berechtigungen nutzt.

## Berechtigungen für die NetApp Data Classification anzeigen

Aktionen	Zweck	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
<ul style="list-style-type: none"><li>• compute.subnetworks.use</li><li>• compute.subnetworks.useExternally</li><li>• compute.instances.addAccessConfig</li></ul>	So aktivieren Sie die NetApp Data Classification.	Ja	Nein	Nein

## Änderungsprotokoll

Die hinzugefügten und entfernten Berechtigungen sind unten aufgeführt.

### 09. Februar 2026

Die `compute.forwardingRules.update`-Berechtigung wurde hinzugefügt, um Infrastructure Manager in Cloud Volumes ONTAP-Bereitstellungen in Google Cloud zu unterstützen.

### 8. Dezember 2025

NetApp wechselt von Google Cloud Deployment Manager zu Google Cloud Infrastructure Manager (IM), um den Console-Agenten in Google Cloud bereitzustellen und auszuführen. Um diese Änderung zu unterstützen, wurden die folgenden Berechtigungen hinzugefügt.

Für den Google Cloud-Nutzer, der den Agenten bereitstellt, sind folgende zusätzliche Berechtigungen erforderlich:

- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
- iam.serviceAccount.actAs
- config.deployments.create
- config.operations.get

Für das Dienstkonto in Google Cloud, das für den täglichen Betrieb verwendet wird, sind folgende zusätzliche Berechtigungen erforderlich:

- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- config.artifacts.import
- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.previews.upload
- config.revisions.getState
- logging.logEntries.create
- storage.objects.create
- storage.objects.delete
- storage.objects.update
- iam.serviceAccounts.get

Für die Bereitstellung von Cloud Volumes ONTAP sind folgende zusätzliche Berechtigungen erforderlich:

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

Für das Dienstkonto, das für den täglichen Betrieb von Cloud Volumes ONTAP verwendet wird, sind die folgenden zusätzlichen Berechtigungen erforderlich.

- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.setLabels

- compute.addresses.useInternal
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.instances.use
- compute.regionBackendServices.delete
- compute.regionBackendServices.update
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- logging.logEntries.route
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- config.operations.get

## **26. November 2025**

Die Berechtigungen wurden aktualisiert, um ihre Verwendung klarer zu gestalten; es wurden jedoch keine Berechtigungen hinzugefügt oder entfernt. Es wurden drei Spalten hinzugefügt, um anzuzeigen, ob die jeweilige Berechtigung für die Bereitstellung, den täglichen Betrieb oder die Löschung verwendet wird. Darüber hinaus sind einige Berechtigungen nach ihrer Verwendung für NetApp Data Classification und NetApp Backup and Recovery getrennt.

## **06. Februar 2023**

Die folgende Berechtigung wurde dieser Richtlinie hinzugefügt:

- compute.instances.updateNetworkInterface

Diese Berechtigung ist für Cloud Volumes ONTAP erforderlich.

**27.01.2023**

Folgende Berechtigungen wurden dieser Richtlinie hinzugefügt:

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Diese Berechtigungen sind für NetApp Backup and Recovery erforderlich.

## Agent-Firewallregeln in Google Cloud

Die Google Cloud-Firewallregeln für den Agenten erfordern sowohl eingehende als auch ausgehende Regeln. Die NetApp Console erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Konsolenagenten aus der Konsole erstellen. Für andere Installationsoptionen müssen Sie diese Sicherheitsgruppe manuell einrichten.

### Eingehende Regeln

Protokoll	Hafen	Zweck
SSH	22	Bietet SSH-Zugriff auf den Agent-Host
HTTP	80	<ul style="list-style-type: none"><li>• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche</li><li>• Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet</li></ul>
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Bietet Cloud Volumes ONTAP Internetzugang. Sie müssen diesen Port nach der Bereitstellung manuell öffnen.

### Ausgangsregeln

Die vordefinierten Firewall-Regeln des Agenten öffnen den gesamten ausgehenden Datenverkehr. Befolgen Sie die grundlegenden Ausgangsregeln, sofern dies akzeptabel ist, oder verwenden Sie erweiterte Ausgangsregeln für strengere Anforderungen.

### Grundlegende Ausgangsregeln

Die vordefinierten Firewall-Regeln für den Agenten umfassen die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr



## Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Agenten erforderlich sind.



Die Quell-IP-Adresse ist der Agent-Host.

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster-Management-LIF	API-Aufrufe an Google Cloud, an ONTAP, an NetApp Data Classification und Senden von AutoSupport -Nachrichten an NetApp
API-Aufrufe	TCP	8080	Datenklassifizierung	Testen der Datenklassifizierung sinstanz während der Bereitstellung
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Datenklassifizierung verwendet

## Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.