Google Cloud permissions and required firewall rules

NetApp Console setup and administration

NetApp
February 11, 2026

Table of Contents

Google Cloud permissions and required firewall rules

Google Cloud permissions for the Console agent

The Console agent requires permissions to perform actions in Google Cloud. These permissions are included in a custom role provided by NetApp. You should understand what the agent does with these permissions.

Google Cloud user account permissions

The custom role below gives a Google Cloud user the permissions needed to deploy an agent. Apply this custom role to the user who will deploy the agent.

View Google Cloud user account permissions

```
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
```

Service account permissions

The custom role below gives the Google Cloud service account attached to the Console agent the permissions needed to manage resources and processes in your Google Cloud network.

Apply this custom role to a service account attached to the Console agent VM.

- Set up Google Cloud permissions for standard mode
- Set up permissions for restricted mode

View Google service account permissions

Ensure the role is up to date as new permissions are added or removed in subsequent releases. The change log lists any required new permissions. Review the Google permissions change log Review how to add Google Cloud service accounts

```
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
```

How Google Cloud permissions are used

The Console agent uses the permissions in the custom role to manage Cloud Volumes ONTAP resources and NetApp data services processes in your Google Cloud network. The following sections describe how the agent uses these permissions.

Permissions used for Cloud Volumes ONTAP

The Console agent uses the permissions in the custom role to manage Cloud Volumes ONTAP resources and processes in your Google Cloud network. The following sections describe how the agent uses these permissions.

Permissions for Cloud Volumes ONTAP

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
config.deployments.create	To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Infrastructure Manager.	Yes	No	No
config.deployments.delete		No	No	Yes
config.deployments.deleteState		No	No	Yes
config.deployments.get		No	Yes	No
config.deployments.getLock		No	Yes	No
config.deployments.getState		No	Yes	No
config.deployments.list		No	Yes	No
config.deployments.lock		No	Yes	No
config.deployments.update		No	Yes	No
config.deployments.updateState		No	Yes	No
config.operations.get		No	Yes	No
config.previews.get		No	Yes	No
config.previews.list		No	Yes	No
config.resources.list		No	Yes	No
config.revisions.get		No	Yes	No
compute.disks.create	To create and manage disks for Cloud Volumes ONTAP.	Yes	Yes	No
compute.disks.createSnapshot		No	Yes	No
compute.disks.delete		No	Yes	Yes
compute.disks.get		No	Yes	No
compute.disks.list		Yes	Yes	No
compute.disks.setLabels		Yes	Yes	No
compute.disks.use		No	Yes	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
compute.firewalls.create	To create firewall rules for Cloud Volumes ONTAP.	Yes	No	No
compute.firewalls.delete		No	Yes	Yes
compute.firewalls.get		Yes	Yes	No
compute.firewalls.list		Yes	Yes	No
compute.forwardingRules.create	Create forwarding rules for traffic routing to backend services.	No	Yes	No
compute.forwardingRules.delete	Delete existing forwarding rules.	No	Yes	No
compute.forwardingRules.get	Retrieve details about existing forwarding rules.	No	Yes	No
compute.forwardingRules.setLabels	Set or update labels on forwarding rules for organization.	No	Yes	No
compute.forwardingRules.update	Update existing forwarding rules for traffic management.	No	Yes	No
compute.globalOperations.get	To get the status of operations.	Yes	Yes	No
compute.healthChecks.create	Create and manage health checks to monitor backend service health.	No	Yes	No
compute.healthChecks.delete		No	Yes	No
compute.healthChecks.get		No	Yes	No
compute.healthChecks.useReadOnly		No	Yes	No
compute.images.get	To get images for VM instances.	Yes	No	No
compute.images.getFromFamily		Yes	No	No
compute.images.list		Yes	No	No
compute.images.useReadOnly		Yes	No	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
compute.instances.attachDisk	To attach and detach disks to Cloud Volumes ONTAP.	Yes	Yes	No
compute.instances.detachDisk		No	Yes	Yes
compute.instances.create	To create and delete Cloud Volumes ONTAP VM instances.	Yes	No	No
compute.instances.delete		No	No	Yes
compute.instances.get	To list VM instances.	Yes	Yes	No
compute.instances.getSerialPortOutput	To get console logs.	Yes	Yes	No
compute.instances.list	To retrieve the list of instances in a zone.	Yes	Yes	No
compute.instances.setDeletionProtection	To set deletion protection on the instance.	Yes	No	No
compute.instances.setLabels	To add labels.	Yes	No	No
compute.instances.setMachineType	To change the machine type for Cloud Volumes ONTAP.	Yes	Yes	No
compute.instances.setMinCpuPlatform		Yes	Yes	No
compute.instances.setMetadata	To add metadata.	Yes	Yes	No
compute.instances.setTags	To add tags for firewall rules.	Yes	Yes	No
compute.instances.start	To start and stop Cloud Volumes ONTAP.	Yes	Yes	No
compute.instances.stop		Yes	Yes	No
compute.instances.updateDisplayDevice		Yes	Yes	No
compute.instances.use	Use virtual machine instances (start, stop, connect operations).	No	Yes	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
compute.machineTypes.get	To get the numbers of cores to check quotas.	Yes	No	No
compute.projects.get	To support multi-projects.	Yes	No	No
compute.resourcePolicies.create	Create and manage resource policies for automated resource management.	No	Yes	No
compute.resourcePolicies.delete		No	Yes	No
compute.resourcePolicies.get		No	Yes	No
compute.snapshots.create	To create and manage persistent disk snapshots.	Yes	Yes	No
compute.snapshots.delete		No	Yes	Yes
compute.snapshots.get		No	Yes	No
compute.snapshots.list		No	Yes	No
compute.snapshots.setLabels		Yes	Yes	No
compute.networks.get	To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance.	Yes	Yes	No
compute.networks.list		Yes	Yes	No
compute.regions.get		Yes	Yes	No
compute.regions.list		Yes	Yes	No
compute.subnetworks.get		Yes	Yes	No
compute.subnetworks.list		Yes	Yes	No
compute.zoneOperations.get		Yes	Yes	No
compute.zones.get		Yes	Yes	No
compute.zones.list		Yes	Yes	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
deploymentmanager.compositeTypes.get	To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager.	Yes	No	No
deploymentmanager.compositeTypes.list		Yes	No	No
deploymentmanager.deployments.create		Yes	No	No
deploymentmanager.deployments.delete		Yes	No	No
deploymentmanager.deployments.get		Yes	No	No
deploymentmanager.deployments.list		Yes	No	No
deploymentmanager.manifests.get		Yes	No	No
deploymentmanager.manifests.list		Yes	No	No
deploymentmanager.operations.get		Yes	No	No
deploymentmanager.operations.list		Yes	No	No
deploymentmanager.resources.get		Yes	No	No
deploymentmanager.resources.list		Yes	No	No
deploymentmanager.typeProviders.get		Yes	No	No
deploymentmanager.typeProviders.list		Yes	No	No
deploymentmanager.types.get		Yes	No	No
deploymentmanager.types.list		Yes	No	No
logging.logEntries.list	To get stack log drives.	Yes	Yes	No
logging.privateLogEntries.list		Yes	Yes	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
logging.logEntries.create	Create and route log entires for monitoring, debugging, and auditing.	Yes	Yes	No
logging.logEntries.route		Yes	Yes	No
resourcemanager.projects.get	To support multi-projects.	Yes	Yes	No
storage.buckets.create	To create and manage a Google Cloud Storage bucket for data tiering.	Yes	Yes	No
storage.buckets.delete		No	Yes	Yes
storage.buckets.get		No	Yes	No
storage.buckets.list		No	Yes	No
storage.buckets.update		No	Yes	No
cloudkms.cryptoKeyVersions.useToEncrypt	To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP.	Yes	Yes	No
cloudkms.cryptoKeys.get		Yes	Yes	No
cloudkms.cryptoKeys.list		Yes	Yes	No
cloudkms.keyRings.list		Yes	Yes	No
cloudbuild.builds.get		Yes	No	No
compute.instances.setServiceAccount	To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket.	Yes	Yes	No
iam.serviceAccounts.actAs		Yes	No	No
iam.serviceAccounts.create		Yes	No	No
iam.serviceAccounts.getIamPolicy		Yes	Yes	No
iam.serviceAccounts.list		Yes	Yes	No
iam.serviceAccountKeys.create		Yes	No	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
storage.objects.create	Create and manage objects (files) in Google Cloud Storage bucket.	Yes	Yes	No
storage.objects.delete		No	No	Yes
storage.objects.get		Yes	Yes	No
storage.objects.list		Yes	Yes	No
compute.addresses.list	To retrieve the addresses in a region when deploying an HA pair.	Yes	No	No
compute.addresses.createInternal	Create internal IP addresses within VPC network for resource allocation.	No	Yes	No
compute.addresses.deleteInternal	Delete internal IP addresses for resource cleanup.	No	Yes	No
compute.addresses.setLabels	Update labels on Address resource.	No	Yes	No
compute.addresses.useInternal	Use internal IP addresses for network communication.	No	Yes	No
compute.backendServices.create	To configure a backend service for distributing traffic in an HA pair.	Yes	No	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
compute.regionBackendServices.create	Create and manage backend services for traffic routing.	Yes	No	No
compute.regionBackendServices.delete		No	Yes	No
compute.regionBackendServices.get		Yes	No	No
compute.regionBackendServices.update		Yes	Yes	No
compute.regionBackendServices.list		Yes	No	No
compute.regionBackendServices.use		No	Yes	No
compute.networks.updatePolicy	To apply firewall rules on the VPCs and subnets for an HA pair.	Yes	No	No
compute.instanceGroups.get	To create and manage storage VMs on Cloud Volumes ONTAP HA pairs.	Yes	Yes	No
compute.addresses.get		Yes	Yes	No
compute.instances.updateNetworkInterface		Yes	Yes	No
compute.instanceGroups.create		No	Yes	No
compute.instanceGroups.delete		No	Yes	No
compute.instanceGroups.update		No	Yes	No
compute.instanceGroups.use		No	Yes	No
monitoring.timeSeries.list	To discover information about Google Cloud Storage buckets.	Yes	Yes	No
storage.buckets.getIamPolicy		Yes	Yes	No

Permissions used for NetApp Backup and Recovery

The Console agent uses the permissions in the custom role to manage NetApp Backup and Recovery resources and processes in your Google Cloud network. The following sections describe how the agent uses these permissions.

View permissions for NetApp Backup and Recovery

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.list • cloudkms.cryptoKeys.setIamPolicy • cloudkms.keyRings.get • cloudkms.keyRings.getIamPolicy • cloudkms.keyRings.list • cloudkms.keyRings.setIamPolicy	To select your own customer-managed keys in the NetApp Backup and Recovery activation wizard instead of using the default Google-managed encryption keys.	Yes	Yes	No

Permissions used for NetApp Data Classification

The Console agent uses the permissions in the custom role to manage NetApp Data Classification resources and processes in your Google Cloud network. The following sections describe how the agent uses these permissions.

View permissions for NetApp Data Classification

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
• compute.subnetworks.use • compute.subnetworks.useExternalIp • compute.instances.addAccessConfig	To enable NetApp Data Classification.	Yes	No	No

Change log

Added and removed permissions are noted below.

09 February 2026

The `compute.forwardingRules.update` permission is added for supporting Infrastructure Manager in Cloud Volumes ONTAP deployments in Google Cloud.

08 December 2025

NetApp is moving from Google Cloud Deployment Manager to Google Cloud Infrastructure Manager (IM) to deploy and run the Console agent in Google Cloud. The following permissions were added to support this change.

The following added permissions are required for the Google Cloud user who deploys the agent:

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

The following additional permissions are required for the service account in Google Cloud used for day-to-day operations:

- 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

The following added permissions are required to deploy Cloud Volumes ONTAP:

- 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

The following added permissions are required for the service account used for day-to-day operations of Cloud Volumes ONTAP.

- 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

The permissions are updated to add clarity about their usage, but no permissions were added or removed. Three columns are added to indicate whether each permission is used for deployment, daily operations, or deletion. Apart from this, a few permissions are segregated based on their use for NetApp Data Classification and NetApp Backup and Recovery.

06 February 2023

The following permission was added to this policy:

- compute.instances.updateNetworkInterface

This permission is required for Cloud Volumes ONTAP.

27 January, 2023

The following permissions were added to this policy:

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

These permissions are required for NetApp Backup and Recovery.

Agent firewall rules in Google Cloud

The Google Cloud firewall rules for the agent requires both inbound and outbound rules. The NetApp Console automatically creates this security group when you create a Console agent from the Console. for other installation options, you need to set up this security group manually.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the agent host
HTTP	80	• Provides HTTP access from client web browsers to the local user interface • Used during the Cloud Volumes ONTAP upgrade process
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides Cloud Volumes ONTAP with internet access. You must manually open this port after deployment.

Outbound rules

The agent's predefined firewall rules open all outbound traffic. Follow basic outbound rules if acceptable, or use advanced outbound rules for stricter requirements.

Basic outbound rules

The predefined firewall rules for the agent include the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the agent.

The source IP address is the agent host.

Service	Protocol	Port	Destination	Purpose
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to Google Cloud, to ONTAP, to NetApp Data Classification, and sending AutoSupport messages to NetApp
API calls	TCP	8080	Data Classification	Probe to Data Classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by Data Classification

Copyright information

Trademark information