# Get started in Google Cloud

## Cloud Volumes ONTAP

NetApp
February 17, 2026

# Table of Contents

# Get started in Google Cloud

## Quick start for Cloud Volumes ONTAP in Google Cloud

Get started with Cloud Volumes ONTAP in Google Cloud in a few steps.

### 1 Create a Console agent

If you don't have a Console agent yet, you need to create one. Learn how to create a Console agent in Google Cloud

Note that if you want to deploy Cloud Volumes ONTAP in a subnet where no internet access is available, then you need to manually install the Console agent and access the NetApp Console that's running on that Console agent. Learn how to manually install the Console agent in a location without internet access

### 2 Plan your configuration

The Console offers preconfigured packages that match your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

Learn more about planning your configuration.

### 3 Set up your networking

a. Ensure that your VPC and subnets will support connectivity between the Console agent and Cloud Volumes ONTAP.

b. If you plan to enable data tiering, configure the Cloud Volumes ONTAP subnet for Private Google Access.

c. If you're deploying an HA pair, ensure that you have four VPCs, each with their own subnet.

d. If you're using a shared VPC, provide the *Compute Network User* role to the Console agent service account.

e. Enable outbound internet access from the target VPC for NetApp AutoSupport.

   This step isn't required if you're deploying Cloud Volumes ONTAP in a location where no internet access is available.

Learn more about networking requirements.

### 4 Set up a service account

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable data tiering to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the NetApp Backup and Recovery to back up volumes to low-cost object storage.

You can set up one service account and use it for both purposes. The service account must have the **Storage Admin** role.

Read step-by-step instructions.

### 5 Enable Google Cloud APIs

Enable the following Google Cloud APIs in your project. These APIs are required to deploy the Console agent and Cloud Volumes ONTAP.

- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Resource Manager API
- Compute Engine API
- Identity and Access Management (IAM) API

### 6 Launch Cloud Volumes ONTAP using the Console

Click **Add System**, select the type of system that you would like to deploy, and complete the steps in the wizard. Read step-by-step instructions.

**Related links**

- Creating a Console agent
- Installing the Console agent software on a Linux host
- Google Cloud permissions for the Console agent

# Plan your Cloud Volumes ONTAP configuration in Google Cloud

When you deploy Cloud Volumes ONTAP in Google Cloud, you can choose a preconfigured system that matches your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

## Choose a Cloud Volumes ONTAP license

Several licensing options are available for Cloud Volumes ONTAP. Each option enables you to choose a consumption model that meets your needs.

- Learn about licensing options for Cloud Volumes ONTAP
- Learn how to set up licensing

## Choose a supported region

Cloud Volumes ONTAP is supported in most Google Cloud regions. View the full list of supported regions.

## Choose a supported machine type

Cloud Volumes ONTAP supports several machine types, depending on the license type that you choose.

Supported configurations for Cloud Volumes ONTAP in Google Cloud

## Understand storage limits

The raw capacity limit for a Cloud Volumes ONTAP system is tied to the license. Additional limits impact the size of aggregates and volumes. You should be aware of these limits as you plan your configuration.

Storage limits for Cloud Volumes ONTAP in Google Cloud

## Size your system in Google Cloud

Sizing your Cloud Volumes ONTAP system can help you meet requirements for performance and capacity. You should be aware of a few key points when choosing a machine type, disk type, and disk size:

### Machine type

Look at the supported machine types in the Cloud Volumes ONTAP Release Notes and then review details from Google about each supported machine type. Match your workload requirements to the number of vCPUs and memory for the machine type. Note that each CPU core increases networking performance.

Refer to the following for more details:

- Google Cloud documentation: N1 standard machine types
- Google Cloud documentation: Performance

### Disk types

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses for a disk. The disk type can be any of the following:

- *Zonal SSD persistent disks*: SSD persistent disks are best for workloads that require high rates of random IOPS.
- *Zonal Balanced persistent disks*: These SSDs balance performance and cost by providing lower IOPS per GB.
- *Zonal Standard persistent disks* : Standard persistent disks are economical and can handle sequential read/write operations.

  For more details, refer to the Google Cloud documentation: Zonal Persistent disks (Standard and SSD).

### Disk size

You need to choose an initial disk size when you deploy a Cloud Volumes ONTAP system. After that you can let the NetApp Console manage a system's capacity for you, but if you want to build aggregates yourself, be aware of the following:

- All disks in an aggregate must be the same size.
- Determine the space that you need, while taking performance into consideration.
- The performance of persistent disks scales automatically with disk size and the number of vCPUs available to the system.

  Refer to the following for more details:

  - Google Cloud documentation: Zonal Persistent disks (Standard and SSD)
  - Google Cloud documentation: Optimizing Persistent Disk and Local SSD Performance

## View default system disks

In addition to the storage for user data, the Console also purchases cloud storage for Cloud Volumes ONTAP system data (boot data, root data, core data, and NVRAM). For planning purposes, it might help for you to review these details before you deploy Cloud Volumes ONTAP.

- View the default disks for Cloud Volumes ONTAP system data in Google Cloud.
- Google Cloud docs: Cloud Quotas overview

  Google Cloud Compute Engine enforces quotas on resource usage so you should ensure that you haven't reached your limit before you deploy Cloud Volumes ONTAP.

The Console agent also requires a system disk. View details about the Console agent's default configuration.

## Collect networking information

When you deploy Cloud Volumes ONTAP in Google Cloud, you need to specify details about your virtual network. You can use a worksheet to collect the information from your administrator.

### Network information for a single-node system

| Google Cloud information | Your value |
|---|---|
| Region | |
| Zone | |
| VPC network | |
| Subnet | |
| Firewall policy (if using your own) | |

### Network information for an HA pair in multiple zones

| Google Cloud information | Your value |
|---|---|
| Region | |
| Zone for Node 1 | |
| Zone for Node 2 | |
| Zone for the mediator | |
| VPC-0 and subnet | |
| VPC-1 and subnet | |
| VPC-2 and subnet | |
| VPC-3 and subnet | |
| Firewall policy (if using your own) | |

**Network information for an HA pair in a single zone**

| Google Cloud information | Your value |
|---|---|
| Region | |
| Zone | |
| VPC-0 and subnet | |
| VPC-1 and subnet | |
| VPC-2 and subnet | |
| VPC-3 and subnet | |
| Firewall policy (if using your own) | |

## Choose a write speed

The Console enables you to choose a write speed setting for Cloud Volumes ONTAP, except for high-availability (HA) pairs in Google Cloud. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and recommendations when using high write speed. Learn more about write speed.

## Choose a volume usage profile

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. When you create a volume in the Console, you can choose a profile that enables these features or a profile that disables them. You should learn more about these features to help you decide which profile to use.

NetApp storage efficiency features provide the following benefits:

**Thin provisioning**

Presents more logical storage to hosts or users than you actually have in your physical storage pool. Instead of preallocating storage space, storage space is allocated dynamically to each volume as data is written.

**Deduplication**

Improves efficiency by locating identical blocks of data and replacing them with references to a single shared block. This technique reduces storage capacity requirements by eliminating redundant blocks of data that reside in the same volume.

**Compression**

Reduces the physical capacity required to store data by compressing data within a volume on primary, secondary, and archive storage.

# Set up Google Cloud networking for Cloud Volumes ONTAP

The NetApp Console handles the set up of networking components for Cloud Volumes ONTAP, such as IP addresses, netmasks, and routes. You need to make sure that outbound internet access is available, that enough private IP addresses are available, that the right connections are in place, and more.

If you want to deploy an HA pair, you should learn how HA pairs work in Google Cloud.

## Requirements for Cloud Volumes ONTAP

The following requirements must be met in Google Cloud.

### Requirements specific to single-node systems

If you want to deploy a single-node system, ensure that your networking meets the following requirements.

#### One VPC

One Virtual Private Cloud (VPC) is required for a single-node system.

#### Private IP addresses

For a single-node system in Google Cloud, the Console allocates private IP addresses to the following:

- Node
- Cluster
- Storage VM
- Data NAS LIF
- Data iSCSI LIF

You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

```
skipSvmManagementLif: true
```

A LIF is an IP address associated with a physical port. A storage VM (SVM) management LIF is required for management tools like SnapCenter.

### Requirements specific to HA pairs

If you want to deploy an HA pair, ensure that your networking meets the following requirements.

#### One or multiple zones

You can ensure the high availability of your data by deploying an HA configuration across multiple or in a single zone. The Console prompts you to choose multiple zones or a single zone when you create the HA pair.

- Multiple zones (recommended)

  Deploying an HA configuration across three zones ensures continuous data availability if a failure occurs within a zone. Note that write performance is slightly lower compared to using a single zone, but it's minimal.

- Single zone

  When deployed in a single zone, a Cloud Volumes ONTAP HA configuration uses a spread placement policy. This policy ensures that an HA configuration is protected from a single point of failure within the zone, without having to use separate zones to achieve fault isolation.

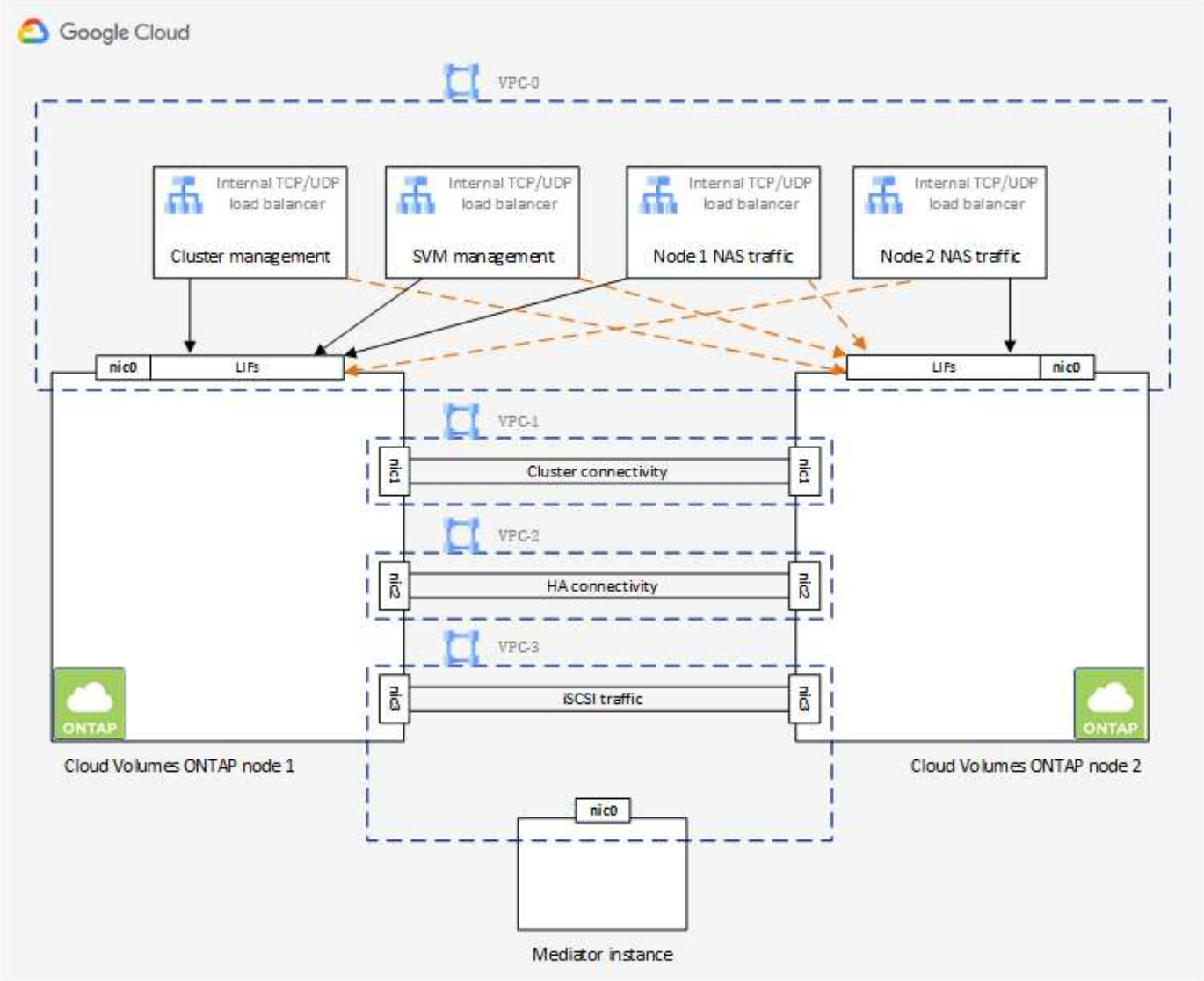
This deployment model does lower your costs because there are no data egress charges between zones.

#### Four Virtual Private Clouds

Four Virtual Private Clouds (VPCs) are required for an HA configuration. Four VPCs are required because Google Cloud requires that each network interface resides in a separate VPC network.

The Console prompts you to choose four VPCs when you create the HA pair:

- VPC-0 for inbound connections to the data and nodes
- VPC-1, VPC-2, and VPC-3 for internal communication between the nodes and the HA mediator




#### Subnets

A private subnet is required for each VPC.

If you place the Console agent in VPC-0, then you will need to enable Private Google Access on the subnet to access the APIs and to enable data tiering.

The subnets in these VPCs must have distinct CIDR ranges. They can’t have overlapping CIDR ranges.

#### Private IP addresses

The Console automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP in Google Cloud. You need to make sure that your networking has enough private addresses available.

The number of LIFs allocated for Cloud Volumes ONTAP depends on whether you deploy a single-node system or an HA pair. A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

- **Single node**
  The Console allocates 4 IP addresses to a single-node system:
  - Node management LIF
  - Cluster management LIF
  - iSCSI data LIF

    An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

  - NAS LIF

    You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

    ```
    skipSvmManagementLif: true
    ```

- **HA pair**
  The Console allocates 12-13 IP addresses to an HA pair:
  - 2 Node management LIFs (e0a)
  - 1 Cluster management LIF (e0a)
  - 2 iSCSI LIFs (e0a)

    An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

  - 1 or 2 NAS LIFs (e0a)
  - 2 Cluster LIFs (e0b)
  - 2 HA Interconnect IP addresses (e0c)
  - 2 RSM iSCSI IP addresses (e0d)

    You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

    ```
    skipSvmManagementLif: true
    ```

#### Internal load balancers

The Console creates four Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the

Cloud Volumes ONTAP HA pair. No setup is required from your end. We've listed this as a requirement simply to inform you of the network traffic and to mitigate any security concerns.

One load balancer is for cluster management, one is for storage VM (SVM) management, one is for NAS traffic to node 1, and the last is for NAS traffic to node 2.

The setup for each load balancer is as follows:

- One shared private IP address
- One global health check

  By default, the ports used by the health check are 63001, 63002, and 63003.

- One regional TCP backend service
- One regional UDP backend service
- One TCP forwarding rule
- One UDP forwarding rule
- Global access is disabled

  Even though global access is disabled by default, enabling it post deployment is supported. We disabled it because cross region traffic will have significantly higher latencies. We wanted to ensure that you didn't have a negative experience due to accidental cross region mounts. Enabling this option is specific to your business needs.

#### Shared VPCs

Cloud Volumes ONTAP and the Console agent are supported in a Google Cloud shared VPC and also in standalone VPCs.

For a single-node system, the VPC can be either a shared VPC or a standalone VPC.

For an HA pair, four VPCs are required. Each of those VPCs can be either shared or standalone. For example, VPC-0 could be a shared VPC, while VPC-1, VPC-2, and VPC-3 could be standalone VPCs.

A shared VPC enables you to configure and centrally manage virtual networks across multiple projects. You can set up shared VPC networks in the *host project* and deploy the Console agent and Cloud Volumes ONTAP virtual machine instances in a *service project*.

Google Cloud documentation: Shared VPC overview.

Review the required shared VPC permissions covered in Console agent deployment

#### Packet mirroring in VPCs

Packet mirroring must be disabled in the Google Cloud subnet in which you deploy Cloud Volumes ONTAP.

#### Outbound internet access

Cloud Volumes ONTAP systems require outbound internet access for accessing external endpoints for various functions. Cloud Volumes ONTAP can't operate properly if these endpoints are blocked in environments with strict security requirements.

The Console agent also contacts several endpoints for day-to-day operations. For information about the

endpoints, refer to View endpoints contacted from the Console agent and Prepare networking for using the Console.

#### Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP uses these endpoints to communicate with various services.

| Endpoints | Applicable for | Purpose | Deployment mode | Impact if endpoint is not available |
|---|---|---|---|---|
| https://netapp-cloud-account.auth0.com | Authentication | Used for authentication in the Console. | Standard and restricted modes. | User authentication fails and the following services remain unavailable:<br>• Cloud Volumes ONTAP services<br>• ONTAP services<br>• Protocols and proxy services |
| https://api.bluexp.netapp.com/tenancy | Tenancy | Used to retrieve Cloud Volumes ONTAP resource from the Console to authorize resources and users. | Standard and restricted modes. | Cloud Volumes ONTAP resources and the users are not authorized. |
| https://mysupport.netapp.com/aods/asupmessage<br>https://mysupport.netapp.com/asupprod/post/1.0/postAsup | AutoSupport | Used to send AutoSupport telemetry data to NetApp support. | Standard and restricted modes. | AutoSupport information remains undelivered. |

| Endpoints | Applicable for | Purpose | Deployment mode | Impact if endpoint is not available |
|---|---|---|---|---|
| https://cloudbuild.googleapis.com/v1 (for only private mode deployments)<br>https://cloudkms.googleapis.com/v1<br>https://cloudresourcemanager.googleapis.com/v1/projects<br>https://compute.googleapis.com/compute/v1<br>https://www.googleapis.com/compute/beta<br>https://www.googleapis.com/compute/v1/projects/<br>https://www.googleapis.com/deploymentmanager/v2/projects<br>https://www.googleapis.com/storage/v1<br>https://www.googleapis.com/upload/storage/v1<br>https://config.googleapis.com/v1<br>https://iam.googleapis.com/v1<br>https://storage.googleapis.com/storage/v1 | Google Cloud (Commercial use). | Communication with Google Cloud services. | Standard, restricted, and private modes. | Cloud Volumes ONTAP cannot communicate with Google Cloud service to perform specific operations for the Console in Google Cloud. |

### Connections to ONTAP systems in other networks

To replicate data between a Cloud Volumes ONTAP system in Google Cloud and ONTAP systems in other networks, you must have a VPN connection between the VPC and the other network—for example, your corporate network.

Google Cloud documentation: Cloud VPN overview.

### Firewall rules

The Console creates Google Cloud firewall rules that include the inbound and outbound rules that Cloud Volumes ONTAP needs to operate successfully. You might want to refer to the ports for testing purposes or if you prefer to use your own firewall rules.

The firewall rules for Cloud Volumes ONTAP requires both inbound and outbound rules. If you're deploying an HA configuration, these are the firewall rules for Cloud Volumes ONTAP in VPC-0.

Note that two sets of firewall rules are required for an HA configuration:

- One set of rules for HA components in VPC-0. These rules enable data access to Cloud Volumes ONTAP.
- Another set of rules for HA components in VPC-1, VPC-2, and VPC-3. These rules are open for inbound & outbound communication between the HA components. Learn more.

Looking for information about the Console agent? View firewall rules for the Console agent

**Inbound rules**

When you add a Cloud Volumes ONTAP system, you can choose the source filter for the predefined firewall policy during deployment:

- **Selected VPC only**: the source filter for inbound traffic is the subnet range of the VPC for the Cloud Volumes ONTAP system and the subnet range of the VPC where the Console agent resides. This is the recommended option.
- **All VPCs**: the source filter for inbound traffic is the 0.0.0.0/0 IP range.

If you use your own firewall policy, ensure that you add all networks that need to communicate with Cloud Volumes ONTAP, but also ensure to add both address ranges to allow the internal Google Load Balancer to function correctly. These addresses are 130.211.0.0/22 and 35.191.0.0/16. For more information, refer to the Google Cloud documentation: Load Balancer Firewall Rules.

| Protocol | Port | Purpose |
|---|---|---|
| All ICMP | All | Pinging the instance |
| HTTP | 80 | HTTP access to the ONTAP System Manager web console using the IP address of the cluster management LIF |
| HTTPS | 443 | Connectivity with the Console agent and HTTPS access to the ONTAP System Manager web console using the IP address of the cluster management LIF |
| SSH | 22 | SSH access to the IP address of the cluster management LIF or a node management LIF |
| TCP | 111 | Remote procedure call for NFS |
| TCP | 139 | NetBIOS service session for CIFS |
| TCP | 161-162 | Simple network management protocol |
| TCP | 445 | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| TCP | 635 | NFS mount |
| TCP | 749 | Kerberos |
| TCP | 2049 | NFS server daemon |
| TCP | 3260 | iSCSI access through the iSCSI data LIF |
| TCP | 4045 | NFS lock daemon |
| TCP | 4046 | Network status monitor for NFS |
| TCP | 10000 | Backup using NDMP |
| TCP | 11104 | Management of intercluster communication sessions for SnapMirror |
| TCP | 11105 | SnapMirror data transfer using intercluster LIFs |
| TCP | 63001-63050 | Load balance probe ports to determine which node is healthy (required for HA pairs only) |
| UDP | 111 | Remote procedure call for NFS |

| Protocol | Port | Purpose |
|---|---|---|
| UDP | 161-162 | Simple network management protocol |
| UDP | 635 | NFS mount |
| UDP | 2049 | NFS server daemon |
| UDP | 4045 | NFS lock daemon |
| UDP | 4046 | Network status monitor for NFS |
| UDP | 4049 | NFS rquotad protocol |

#### Outbound rules

The predefined security group for Cloud Volumes ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

#### Basic outbound rules

The predefined security group for Cloud Volumes ONTAP includes the following outbound rules.

| Protocol | Port | Purpose |
|---|---|---|
| All ICMP | All | All outbound traffic |
| 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 Cloud Volumes ONTAP. The Cloud Volumes ONTAP clusters use the following ports for regulating nodes traffic.

The source is the interface (IP address) of the Cloud Volumes ONTAP system.

| Service | Protocol | Port | Source | Destination | Purpose |
|---|---|---|---|---|---|
| Active Directory | TCP | 88 | Node management LIF | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Node management LIF | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Node management LIF | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Node management LIF | Active Directory forest | NetBIOS service session |
| | TCP & UDP | 389 | Node management LIF | Active Directory forest | LDAP |
| | TCP | 445 | Node management LIF | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Node management LIF | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Node management LIF | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Node management LIF | Active Directory forest | Kerberos V change & set Password (RPCSEC_GSS) |
| | TCP | 88 | Data LIF (NFS, CIFS, iSCSI) | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS service session |
| | TCP & UDP | 389 | Data LIF (NFS, CIFS) | Active Directory forest | LDAP |
| | TCP | 445 | Data LIF (NFS, CIFS) | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (RPCSEC_GSS) |

| Service | Protocol | Port | Source | Destination | Purpose |
|---|---|---|---|---|---|
| AutoSupport | HTTPS | 443 | Node management LIF | mysupport.netapp.com | AutoSupport (HTTPS is the default) |
| | HTTP | 80 | Node management LIF | mysupport.netapp.com | AutoSupport (only if the transport protocol is changed from HTTPS to HTTP) |
| | TCP | 3128 | Node management LIF | Console agent | Sending AutoSupport messages through a proxy server on the Console agent, if an outbound internet connection isn't available |
| Configuration backups | HTTP | 80 | Node management LIF | http://<console-agent-IP-address>/occm/offboxconfig | Send configuration backups to the Console agent. ONTAP documentation |
| DHCP | UDP | 68 | Node management LIF | DHCP | DHCP client for first-time setup |
| DHCPS | UDP | 67 | Node management LIF | DHCP | DHCP server |
| DNS | UDP | 53 | Node management LIF and data LIF (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 18600–18699 | Node management LIF | Destination servers | NDMP copy |
| SMTP | TCP | 25 | Node management LIF | Mail server | SMTP alerts, can be used for AutoSupport |
| SNMP | TCP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | TCP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| SnapMirror | TCP | 11104 | Intercluster LIF | ONTAP intercluster LIFs | Management of intercluster communication sessions for SnapMirror |
| | TCP | 11105 | Intercluster LIF | ONTAP intercluster LIFs | SnapMirror data transfer |
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |

#### Rules for VPC-1, VPC-2, and VPC-3

In Google Cloud, an HA configuration is deployed across four VPCs. The firewall rules needed for the HA configuration in VPC-0 are listed above for Cloud Volumes ONTAP.

Meanwhile, the predefined firewall rules created for the instances in VPC-1, VPC-2, and VPC-3 enable ingress communication over *all* protocols and ports. These rules enable communication between HA nodes.

Communication from the HA nodes to the HA mediator takes place over port 3260 (iSCSI).

> To enable high write speed for new Google Cloud HA pair deployments, a maximum transmission unit (MTU) of at least 8,896 bytes is required for VPC-1, VPC-2, and VPC-3. If you choose to upgrade existing VPC-1, VPC-2, and VPC-3 to an MTU of 8,896 bytes, you must shutdown all existing HA systems using these VPCs during the configuration process.

## Requirements for the Console agent

If you haven't created a Console agent yet, you should review networking requirements.

- View networking requirements for the Console agent
- Firewall rules in Google Cloud

#### Network configurations to support Console agent proxy

You can use the proxy servers configured for the Console agent to enable outbound internet access from Cloud Volumes ONTAP. The Console supports two types of proxies:

- **Explicit proxy**: The outbound traffic from Cloud Volumes ONTAP uses the HTTP address of the proxy server specified during the Console agent proxy configuration. The Console agent administrator might also have configured user credentials and root CA certificates for additional authentication. If a root CA certificate is available for the explicit proxy, make sure to obtain and upload the same certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.
- **Transparent proxy**: The network is configured to automatically route outbound traffic from Cloud Volumes ONTAP through the Console agent proxy. When setting up a transparent proxy, the Console agent administrator needs to provide only a root CA certificate for connectivity from Cloud Volumes ONTAP, not the HTTP address of the proxy server. Make sure that you obtain and upload the same root CA certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

For information about configuring proxy servers for the Console agent, refer to the Configure a Console agent to use a proxy server.

#### Configure network tags for Cloud Volumes ONTAP in Google Cloud

During the transparent proxy configuration of the Console agent, the administrator adds a network tag for Google Cloud. You need to obtain and manually add the same network tag for your Cloud Volumes ONTAP configuration. This tag is necessary for the proxy server to function correctly.

1. In the Google Cloud Console, locate your Cloud Volumes ONTAP system.
2. Go to **Details > Networking > Network tags**.
3. Add the tag used for the Console agent and save the configuration.

#### Related topics

- Verify AutoSupport setup for Cloud Volumes ONTAP

- Learn about ONTAP internal ports.

# Set up VPC Service Controls to deploy Cloud Volumes ONTAP in Google Cloud

When choosing to lock down your Google Cloud environment with VPC Service Controls, you should understand how NetApp Console and Cloud Volumes ONTAP interact with the Google Cloud APIs, as well as how to configure your service perimeter to deploy the Console and Cloud Volumes ONTAP.

VPC Service Controls enable you to control access to Google-managed services outside of a trusted perimeter, to block data access from untrusted locations, and to mitigate unauthorized data transfer risks. Learn more about Google Cloud VPC Service Controls.

## How NetApp services communicate with VPC Service Controls

The Console communicates directly with the Google Cloud APIs. This is either triggered from an external IP address outside of Google Cloud (for example, from api.services.cloud.netapp.com), or within Google Cloud from an internal address assigned to the Console agent.

Depending on the deployment style of the Console agent, certain exceptions may have to be made for your service perimeter.

## Images

Both Cloud Volumes ONTAP and the Console use images from a project within Google Cloud that is managed by NetApp. This can affect the deployment of the Console agent and Cloud Volumes ONTAP, if your organization has a policy that blocks the use of images that are not hosted within the organization.

You can deploy a Console agent manually using the manual installation method, but Cloud Volumes ONTAP will also need to pull images from the NetApp project. You must provide an allowed list in order to deploy a Console agent and Cloud Volumes ONTAP.

### Deploying a Console agent

The user who deploys a Console agent needs to be able to reference an image hosted in the projectId *netapp-cloudmanager* and the project number *14190056516*.

### Deploying Cloud Volumes ONTAP

- The Console service account needs to reference an image hosted in the projectId *netapp-cloudmanager* and the project number *14190056516* from the service project.
- The service account for the default Google APIs Service Agent needs to reference an image hosted in the projectId *netapp-cloudmanager* and the project number *14190056516* from the service project.

Examples of the rules needed for pulling these images with VPC Service Controls are defined below.

## VPC Service Controls perimeter policies

Policies allow exceptions to the VPC Service Controls rule sets. For more information about policies, please visit the Google Cloud VPC Service Controls Policy Documentation.

To set the policies that the Console requires, navigate to your VPC Service Controls Perimeter within your organization and add the following policies. The fields should match the options given in the VPC Service Controls policy page. Also note that **all** rules are required and the **OR** parameters should be used in the rule set.

### Ingress rules

#### Rule 1

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

OR

#### Rule 2

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

OR

**Rule 3**

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

**Egress rules**

**Rule 1:**

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

The project number outlined above is the project *netapp-cloudmanager* used by NetApp to store images for the Console agent and for Cloud Volumes ONTAP.

# Create a Google Cloud service account for Cloud Volumes ONTAP

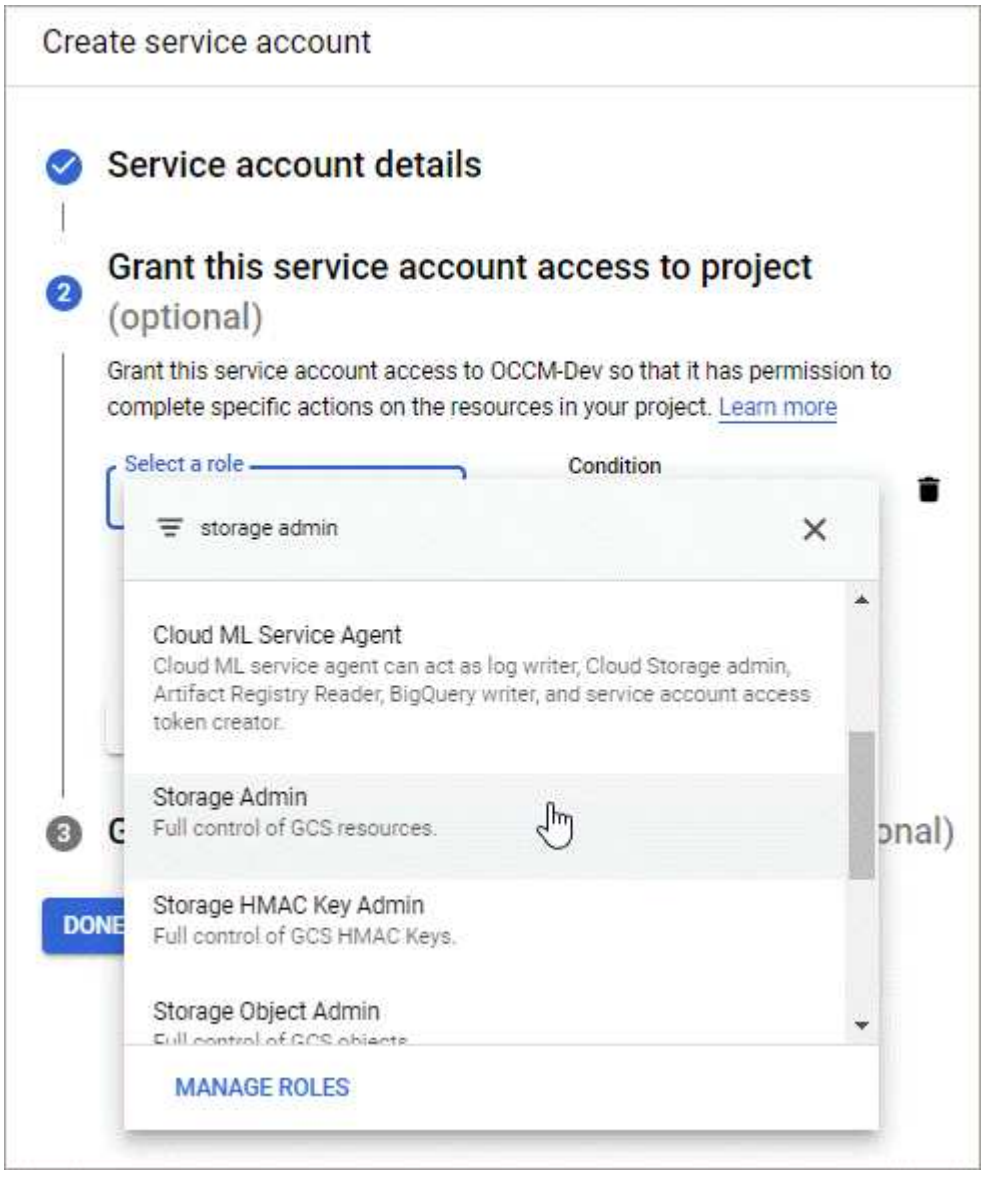
Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable data tiering to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the NetApp Backup and Recovery to back up volumes to low-cost object storage.

Cloud Volumes ONTAP uses the service account to access and manage one bucket for tiered data and another bucket for backups.

You can set up one service account and use it for both purposes. The service account must have the **Storage Admin** role.

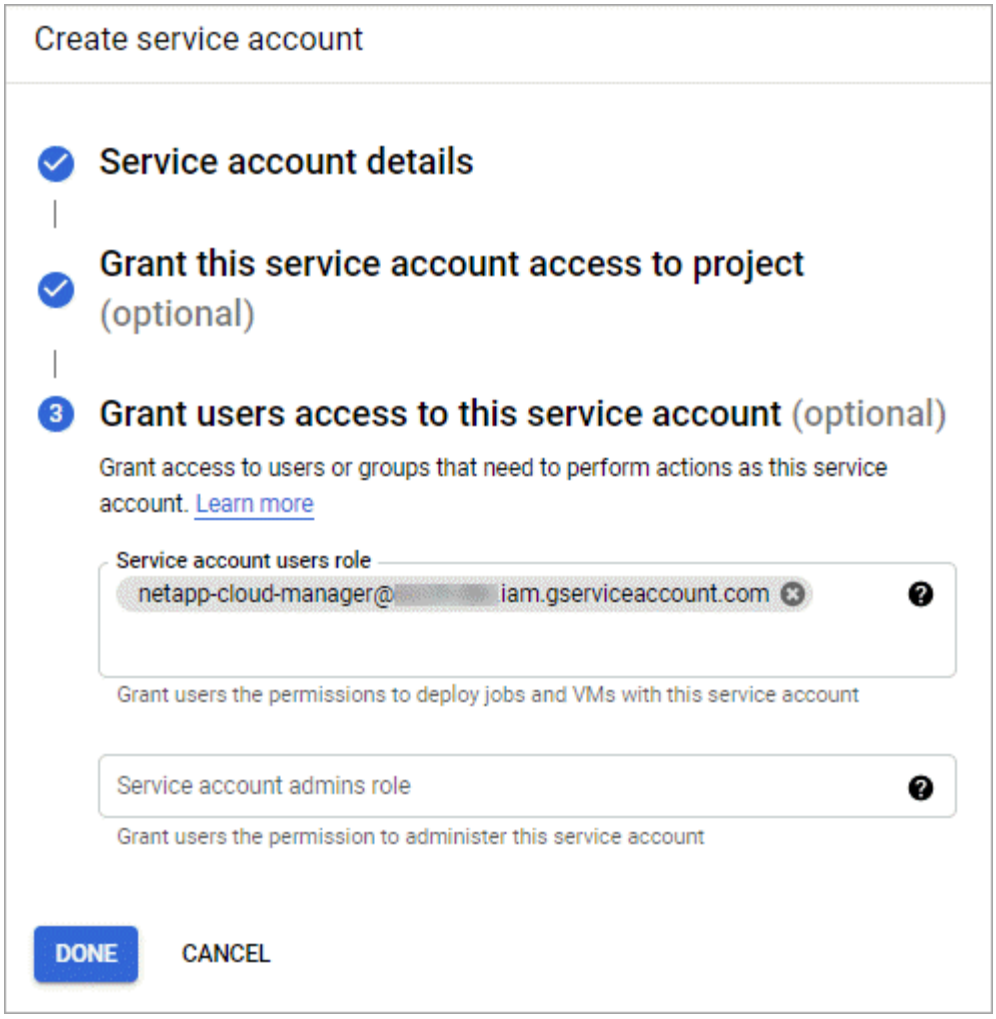
**Steps**

1. In the Google Cloud Console, go to the Service accounts page.
2. Select your project.
3. Click **Create service account** and provide the required information.
   a. **Service account details**: Enter a name and description.
   b. **Grant this service account access to project**: Select the **Storage Admin** role.



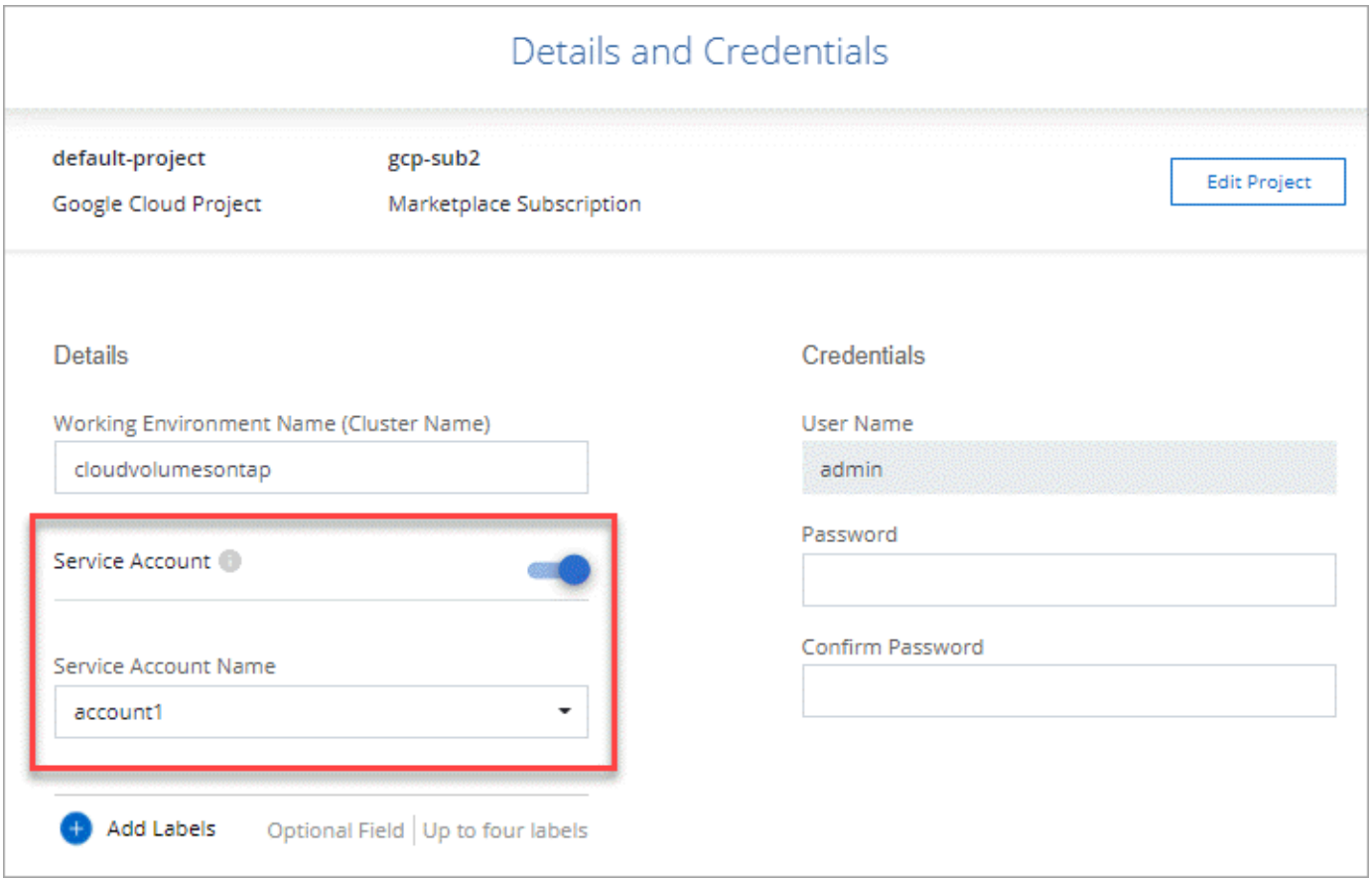

   c. **Grant users access to this service account**: Add the Console agent service account as a *Service Account User* to this new service account.

      This step is required for data tiering only. It's not required for Backup and Recovery.




**What's next?**

You'll need to select the service account later when you create a Cloud Volumes ONTAP system.




# Using customer-managed encryption keys with Cloud Volumes ONTAP

While Google Cloud Storage always encrypts your data before it's written to disk, you can use the APIs to create a Cloud Volumes ONTAP system that uses *customer-managed encryption keys*. These are keys that you generate and manage in GCP using the Cloud Key Management Service.

**Steps**

1. Ensure that the Console agent service account has the correct permissions at the project level, in the project where the key is stored.

   The permissions are provided in the the service account permissions by default, but may not be applied if you use an alternate project for the Cloud Key Management Service.

   The permissions are as follows:

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. Ensure that the service account for the Google Compute Engine Service Agent has Cloud KMS

Encrypter/Decrypter permissions on the key.

The name of the service account uses the following format: "service-[service_project_number]@compute-system.iam.gserviceaccount.com".

Google Cloud Documentation: Using IAM with Cloud KMS - Granting roles on a resource

3. Obtain the "id" of the key by invoking the get command for the `/gcp/vsa/metadata/gcp-encryption-keys` API call or by choosing "Copy Resource Name" on the key in the GCP console.
4. If using customer-managed encryption keys and tiering data to object storage, the NetApp Console attempts to utilize the same keys that are used to encrypt the persistent disks. But you'll first need to enable Google Cloud Storage buckets to use the keys:

   a. Find the Google Cloud Storage service agent by following the Google Cloud Documentation: Getting the Cloud Storage service agent.

   b. Navigate to the encryption key and assign the Google Cloud Storage service agent with Cloud KMS Encrypter/Decrypter permissions.

   For more information, refer to Google Cloud Documentation: Using customer-managed encryption keys

5. Use the "gcpEncryption" parameter with your API request when creating a system.

   **Example**

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

Refer to the NetApp Console automation docs for more details about using the "GcpEncryption" parameter.

# Set up licensing for Cloud Volumes ONTAP in Google Cloud

After you decide which licensing option you want to use with Cloud Volumes ONTAP, a few steps are required before you can choose that licensing option when creating a new system.

## Freemium

Select the Freemium offering to use Cloud Volumes ONTAP free of charge with up to 500 GiB of provisioned capacity. Learn more about the Freemium offering.

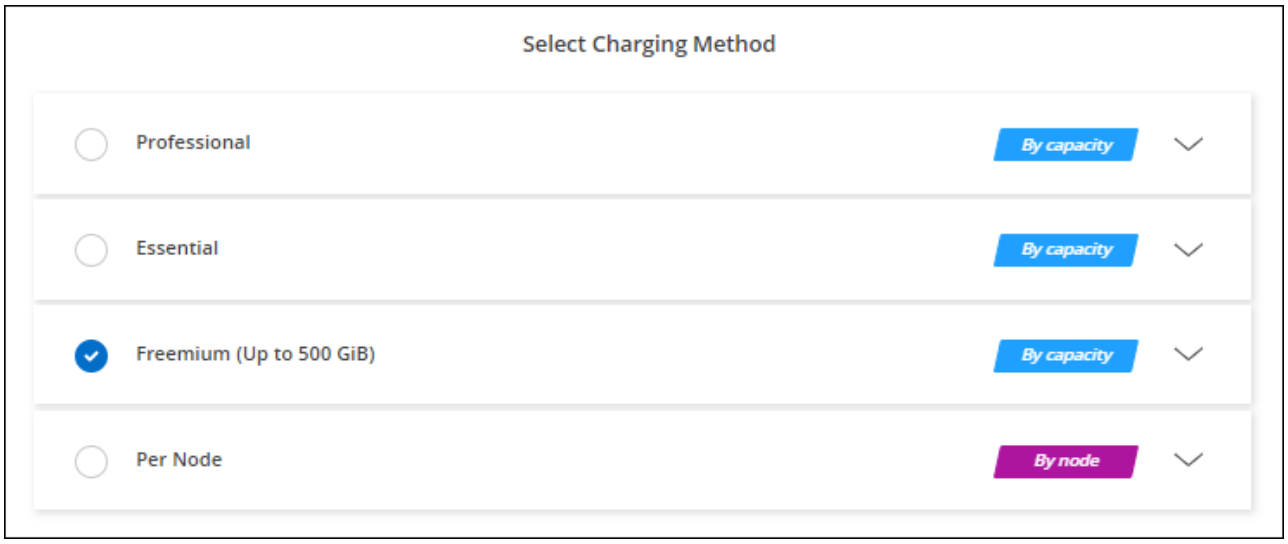
**Steps**

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps in the NetApp Console.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Google Cloud Marketplace.

      You won't be charged through the marketplace subscription unless you exceed 500 GiB of provisioned

capacity, at which time the system is automatically converted to the Essentials package.

b. After you return to the Console, select **Freemium** when you reach the charging methods page.




View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.

## Capacity-based license

Capacity-based licensing enables you to pay for Cloud Volumes ONTAP per TiB of capacity. Capacity-based licensing is available in the form of a *package*: the Essentials or Professional package.

The Essentials and Professional packages are available with the following consumption models or purchase options:

- A license (bring your own license (BYOL)) purchased from NetApp
- An hourly, pay-as-you-go (PAYGO) subscription from the Google Cloud Marketplace
- An annual contract

Learn more about capacity-based licensing.

The following sections describe how to get started with each of these consumption models.

### BYOL

Pay upfront by purchasing a license (BYOL) from NetApp to deploy Cloud Volumes ONTAP systems in any cloud provider.

NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.

**Steps**

1. Contact NetApp Sales to obtain a license
2. Add your NetApp Support Site account to the NetApp Console

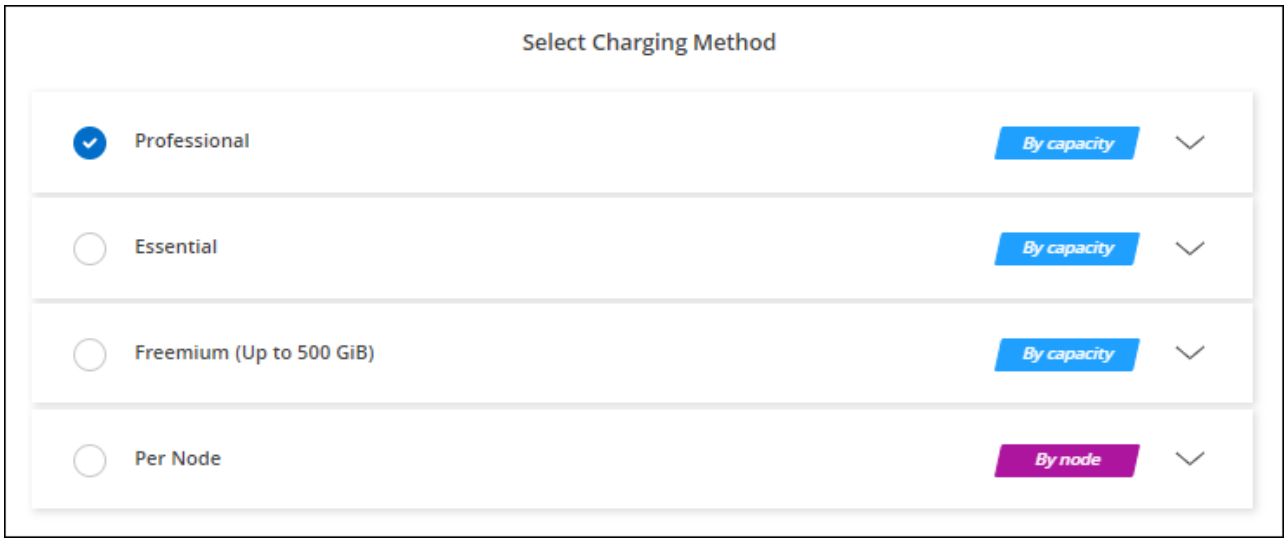
   The Console automatically queries NetApp's licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, the Console adds the licenses.

Your license must be available from the Console before you can use it with Cloud Volumes ONTAP. If needed, you can manually add the license to the Console.

3. On the **Systems** page, click **Add System** and follow the steps.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Google Cloud Marketplace.

      The license that you purchased from NetApp is always charged first, but you'll be charged from the hourly rate in the marketplace if you exceed your licensed capacity or if the term of your license expires.

   b. After you return to the Console, select a capacity-based package when you reach the charging methods page.




View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.

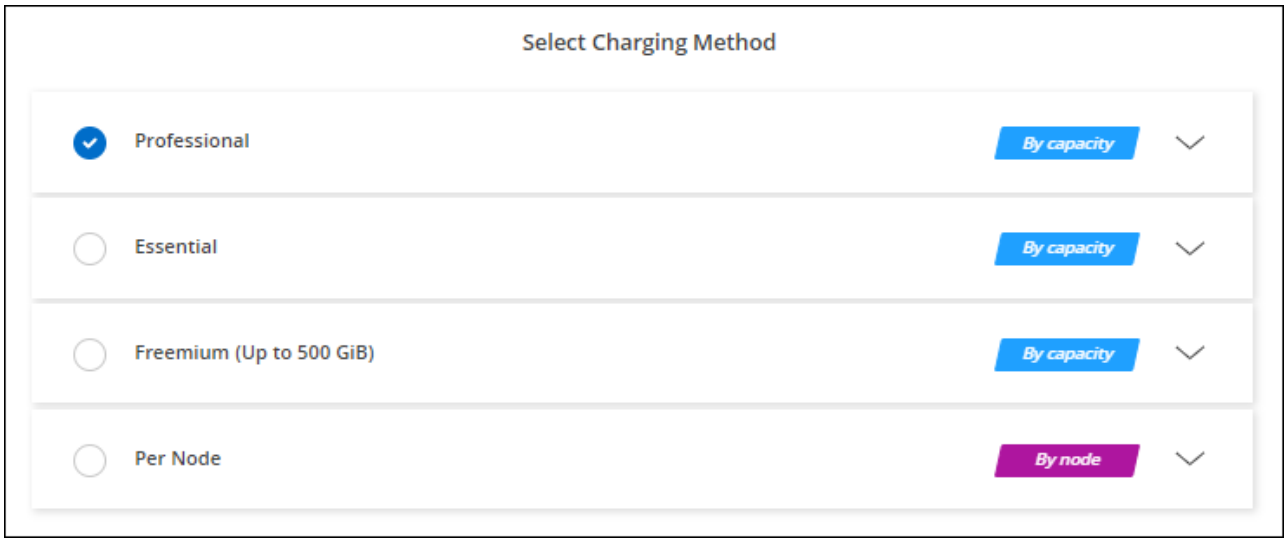
### PAYGO subscription

Pay hourly by subscribing to the offer from your cloud provider's marketplace.

When you create a Cloud Volumes ONTAP system, the Console prompts you to subscribe to the agreement that's available in the Google Cloud Marketplace. That subscription is then associated with the system for charging. You can use that same subscription for additional systems.

#### Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Google Cloud Marketplace.
   b. After you return to the Console, select a capacity-based package when you reach the charging methods page.




View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.

You can manage the Google Cloud Marketplace subscriptions associated with your accounts from the Settings > Credentials page. Learn how to manage your Google Cloud credentials and subscriptions

### Annual contract

Pay for Cloud Volumes ONTAP annually by purchasing an annual contract.

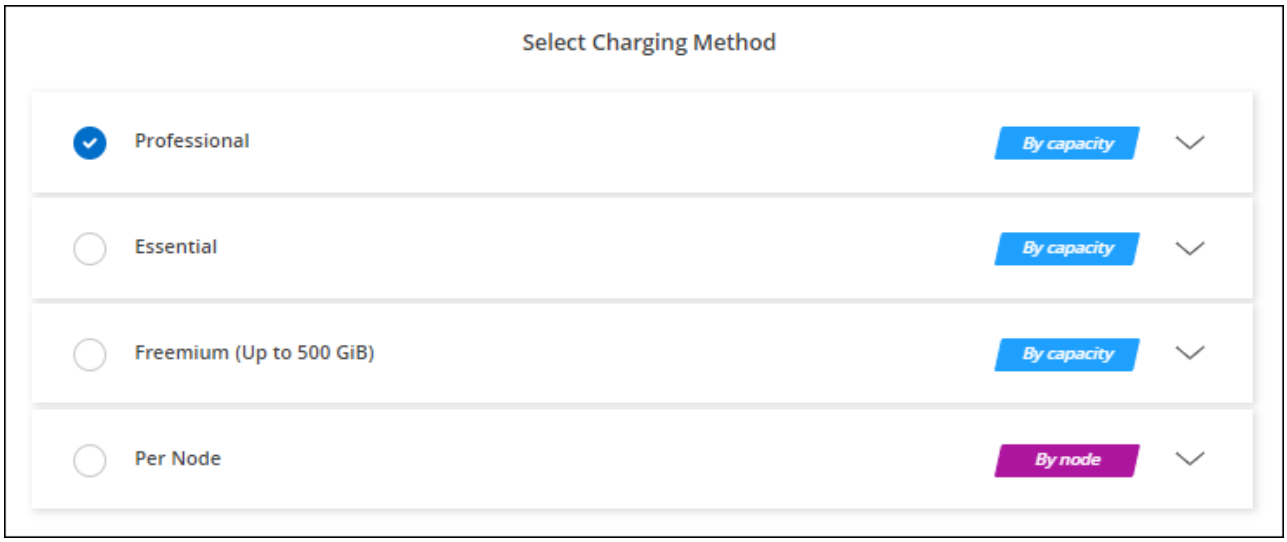
#### Steps

1. Contact your NetApp sales representative to purchase an annual contract.

   The contract is available as a *private* offer in the Google Cloud Marketplace.

   After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Google Cloud Marketplace during system creation.

2. On the **Systems** page, click **Add System** and follow the steps.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the annual plan in the Google Cloud Marketplace.
   b. In Google Cloud, select the annual plan that was shared with your account and then click **Subscribe**.
   c. After you return to the Console, select a capacity-based package when you reach the charging methods page.



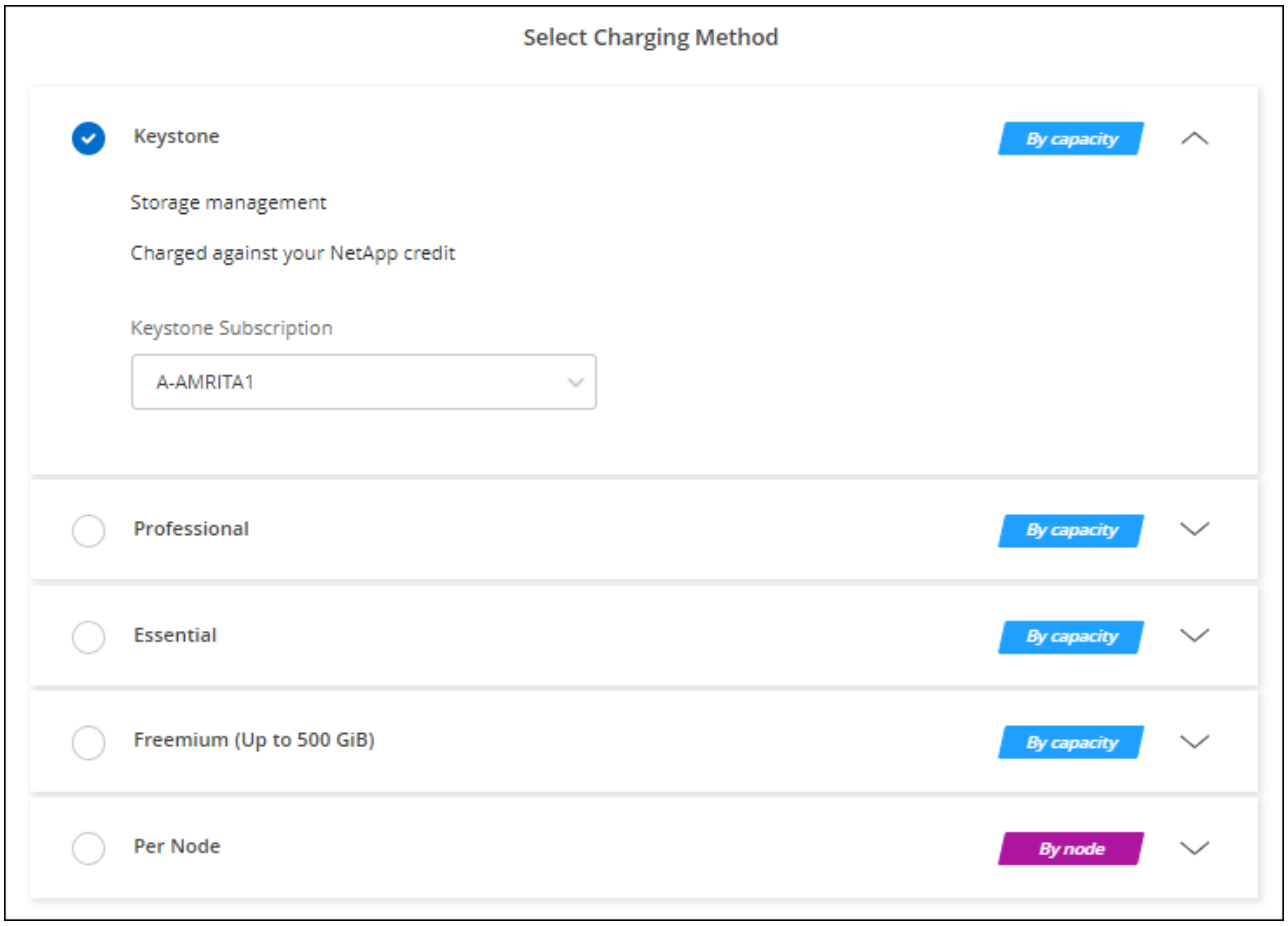

View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.

## Keystone Subscription

A Keystone Subscription is a pay-as-you-grow subscription-based service. Learn more about NetApp Keystone Subscriptions.

**Steps**

1. If you don't have a subscription yet, contact NetApp
2. Contact NetApp to authorize your the Console user account with one or more Keystone Subscriptions.
3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.
4. On the **Systems** page, click **Add System** and follow the steps.
    a. Select the Keystone Subscription charging method when prompted to choose a charging method.




View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.

### Node-based license

A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases. For information, refer to:

- End of availability for node-based licenses
- End of availability of node-based licenses
- Convert a node-based license to a capacity-based license

# Launch Cloud Volumes ONTAP in Google Cloud

You can launch Cloud Volumes ONTAP in a single-node configuration or as an HA pair in Google Cloud.

### Before you begin

You need the following before you begin.

- A NetApp Console agent that's up and running.
  - You should have a Console agent that is associated with your system.

    - You should be prepared to leave the Console agent running at all times.
    - The service account associated with the Console agent should have the required permissions
- An understanding of the configuration that you want to use.

  You should have prepared by choosing a configuration and by obtaining Google Cloud networking information from your administrator. For details, refer to Planning your Cloud Volumes ONTAP configuration.

- An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  Learn how to set up licensing.

- Google Cloud APIs should be enabled in your project:
    - Cloud Deployment Manager V2 API
    - Cloud Logging API
    - Cloud Resource Manager API
    - Compute Engine API
    - Identity and Access Management (IAM) API

## Launch a single-node system in Google Cloud

Create a system in the NetApp Console to launch Cloud Volumes ONTAP in Google Cloud.

**Steps**

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. **Choose a Location**: Select **Google Cloud** and **Cloud Volumes ONTAP**.
4. If you're prompted, create a Console agent.
5. **Details & Credentials**: Select a project, specify a cluster name, optionally select a service account, optionally add labels, and then specify credentials.

   The following table describes fields for which you might need guidance:

| Field | Description |
|---|---|
| System Name | The Console uses the system name to name both the Cloud Volumes ONTAP system and the Google Cloud VM instance. It also uses the name as the prefix for the predefined security group, if you select that option. |
| Service Account Name | If you plan to use data tiering or NetApp Backup and Recovery with Cloud Volumes ONTAP, then you need to enable **Service Account** and select a service account that has the predefined Storage Admin role. Learn how to create a service account. |

| Field | Description |
| --- | --- |
| Add Labels | Labels are metadata for your Google Cloud resources. The Console adds the labels to the Cloud Volumes ONTAP system and Google Cloud resources associated with the system.<br><br>You can add up to four labels from the user interface when creating a system, and then you can add more after it's created. Note that the API does not limit you to four labels when creating a system.<br><br>For information about labels, refer to the Google Cloud Documentation: Labeling Resources. |
| User name and password | These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name. |
| Edit Project | Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where of the Console.<br><br>If you don't see any additional projects in the drop-down list, then you haven't yet associated the service account with other projects. Go to the Google Cloud Console, open the IAM service, and select the project. Add the service account with the role that you use for the Console to that project. You'll need to repeat this step for each project.<br><br>This is the service account that you set up for the Console, as described on this page.<br><br>Click **Add Subscription** to associate the selected credentials with a subscription.<br><br>To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a Google Cloud project that's associated with a subscription to Cloud Volumes ONTAP from the Google Cloud marketplace. Refer to Associating a marketplace subscription with Google Cloud credentials. |

6. **Services**: Select the services that you want to use on this system. In order to select Backup and Recovery, or to use NetApp Cloud Tiering, you must have specified the Service Account in step 3.

   If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

7. **Location & Connectivity**: Select the Google Cloud region and zone for your system, choose a firewall policy, and confirm network connectivity to Google Cloud storage for data tiering.

   The following table describes fields for which you might need guidance:

| Field | Description |
| --- | --- |
| Connectivity verification | To tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access. |
| Generated firewall policy | If you let the Console generate the firewall policy for you, you need to choose how you'll allow traffic:<br>• If you choose **Selected VPC only**, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Console agent resides. This is the recommended option.<br>• If you choose **All VPCs**, the source filter for inbound traffic is the 0.0.0.0/0 IP range. |
| Use existing firewall policy | If you use an existing firewall policy, ensure that it includes the required rules: Learn about firewall rules for Cloud Volumes ONTAP |

8. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account:
   - Learn about licensing options for Cloud Volumes ONTAP
   - Learn how to set up licensing
9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**. The preconfigured packages vary with the selected Cloud Volumes ONTAP version. For example, for Cloud Volumes ONTAP 9.18.1 and later, the Console shows packages with C3 VMs, including Hyperdisk Balanced disks. You can modify the configurations, such as IOPS and throughput parameters, based on your workload needs.

   If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.
10. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a machine type.

    If a newer Release Candidate, General Availability, or patch release is available for a selected version, then the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another— for example, from 9.13 to 9.14.
11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

    The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

    The disk size is for all disks in the initial aggregate and for any additional aggregates that the Console creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

    For help choosing a disk type and size, refer to Size your system in Google Cloud.
12. **Flash Cache, Write Speed & WORM**:

a. Enable **Flash Cache** or choose **Normal** or **High** write speed if you need.

   Learn more about Flash Cache and write speed.

   > ⓘ High write speed and a higher maximum transmission unit (MTU) of 8,896 bytes are available through the **High** write speed option. In addition, the higher MTU of 8,896 requires the selection of VPC-1, VPC-2 and VPC-3 for the deployment. For more information on VPC-1, VPC-2, and VPC-3, refer to Rules for VPC-1, VPC-2, and VPC-3.

b. Activate write once, read many (WORM) storage, if desired.

   WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

   Learn more about WORM storage.

c. If you activate WORM storage, select the retention period.

13. **Data Tiering in Google Cloud Platform**: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then either select a service account that has the predefined Storage Admin role (required for Cloud Volumes ONTAP 9.7 or later), or select a Google Cloud account (required for Cloud Volumes ONTAP 9.6).

    Note the following:

    - The Console sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Console agent service account as a user of the tiering service account, otherwise, you can't select it from the Console.
    - For help with adding a Google Cloud account, refer to Setting up and adding Google Cloud accounts for data tiering with 9.6.
    - You can choose a specific volume tiering policy when you create or edit a volume.
    - If you disable data tiering, you can enable it on subsequent aggregates, but you'll need to turn off the system and add a service account from the Google Cloud Console.

    Learn more about data tiering.

14. **Create Volume**: Enter details for the new volume or click **Skip**.

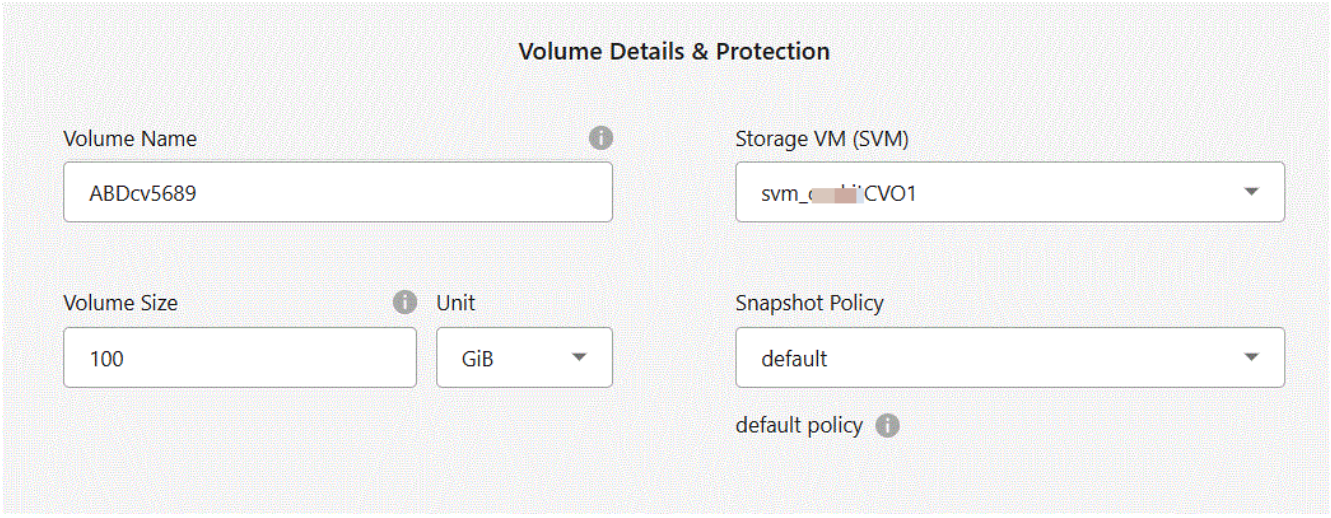
    Learn about supported client protocols and versions.

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

| Field | Description |
|---|---|
| Size | The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it. |
| Access control (for NFS only) | An export policy defines the clients in the subnet that can access the volume. By default, the Console enters a value that provides access to all instances in the subnet. |

| Field | Description |
|---|---|
| Permissions and Users / Groups (for CIFS only) | These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username. |
| Snapshot Policy | A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server. |
| Advanced options (for NFS only) | Select an NFS version for the volume: either NFSv3 or NFSv4. |
| Initiator group and IQN (for iSCSI only) | iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.<br><br>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.<br><br>iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs).<br><br>When you create an iSCSI volume, the Console automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts. |

The following image shows the first page of the volume creation wizard:




15. **CIFS Setup**: If you chose the CIFS protocol, set up a CIFS server.

| Field | Description |
|---|---|
| DNS Primary and Secondary IP Address | The IP addresses of the DNS servers that provide name resolution for the CIFS server.<br>The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.<br><br>If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address. |
| Active Directory Domain to join | The FQDN of the Active Directory (AD) domain that you want the CIFS server to join. |
| Credentials authorized to join the domain | The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain. |
| CIFS server NetBIOS name | A CIFS server name that is unique in the AD domain. |
| Organizational Unit | The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.<br><br>To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field.<br><br>Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD |
| DNS Domain | The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain. |
| NTP Server | Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. For information, refer to the NetApp Console automation docs for details.<br><br>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server. |

16. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and change the volume tiering policy, if needed.

    For more information, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

17. **Review & Approve**: Review and confirm your selections.
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the Google Cloud resources that the Console will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

**Result**

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the **Audit** page.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the system and click **Re-create environment**.

For additional help, go to NetApp Cloud Volumes ONTAP Support.

**After you finish**

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

> After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Google Cloud portal, such as the system tags, and the labels set in the Google Cloud resources. Any changes made to these configurations may lead to unexpected behavior or data loss.

## Launch an HA pair in Google Cloud

Create a system in the Console to launch Cloud Volumes ONTAP in Google Cloud.

**Steps**

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Storage > System** and follow the prompts.
3. **Choose a Location**: Select **Google Cloud** and **Cloud Volumes ONTAP HA**.
4. **Details & Credentials**: Select a project, specify a cluster name, optionally select a Service Account, optionally add labels, and then specify credentials.

   The following table describes fields for which you might need guidance:

| Field | Description |
|---|---|
| System Name | The Console uses the system name to name both the Cloud Volumes ONTAP system and the Google Cloud VM instance. It also uses the name as the prefix for the predefined security group, if you select that option. |
| Service Account Name | If you plan to use the NetApp Cloud Tiering or Backup and Recovery services, you need to enable the **Service Account** switch and then select the Service Account that has the predefined Storage Admin role. |
| Add Labels | Labels are metadata for your Google Cloud resources. The Console adds the labels to the Cloud Volumes ONTAP system and Google Cloud resources associated with the system.<br><br>You can add up to four labels from the user interface when creating a system, and then you can add more after it's created. Note that the API does not limit you to four labels when creating a system.<br><br>For information about labels, refer to Google Cloud Documentation: Labeling Resources. |

| Field | Description |
| --- | --- |
| User name and password | These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name. |
| Edit Project | Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project of the Console.<br><br>If you don't see any additional projects in the drop-down list, then you haven't yet associated the service account with other projects. Go to the Google Cloud Console, open the IAM service, and select the project. Add the service account with the role that you use for the Console to that project. You'll need to repeat this step for each project.<br><br>This is the service account that you set up for the Console, as described on this page.<br><br>Click **Add Subscription** to associate the selected credentials with a subscription.<br><br>To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a Google Cloud project that's associated with a subscription to Cloud Volumes ONTAP from the Google Cloud Marketplace. Refer to Associating a marketplace subscription with Google Cloud credentials. |

5. **Services**: Select the services that you want to use on this system. To select Backup and Recovery, or to use NetApp Cloud Tiering, you must have specified the Service Account in step 3.

   If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

6. **HA Deployment Models**: Choose multiple zones (recommended) or a single zone for the HA configuration. Then select a region and zone.

   Learn more about HA deployment models.

7. **Connectivity**: Select four different VPCs for the HA configuration, a subnet in each VPC, and then choose a firewall policy.

   Learn more about networking requirements.

   The following table describes fields for which you might need guidance:

| Field | Description |
| --- | --- |
| Generated policy | If you let the Console generate the firewall policy for you, you need to choose how you'll allow traffic:<br>• If you choose **Selected VPC only**, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Console agent resides. This is the recommended option.<br>• If you choose **All VPCs**, the source filter for inbound traffic is the 0.0.0.0/0 IP range. |
| Use existing | If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP. |

8. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.
   - Learn about licensing options for Cloud Volumes ONTAP.
   - Learn how to set up licensing.
9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

   If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.

10. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a machine type.

    If a newer Release Candidate, General Availability, or patch release is available for the selected version, then the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.

11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

    The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

    The disk size is for all disks in the initial aggregate and for any additional aggregates that the Console creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

    For help choosing a disk type and size, refer to Size your system in Google Cloud.

12. **Flash Cache, Write Speed & WORM**:
    a. Enable **Flash Cache** or choose **Normal** or **High** write speed if you need.

       Learn more about Flash Cache and write speed.

High write speed and a higher maximum transmission unit (MTU) of 8,896 bytes are available through the **High** write speed option with the n2-standard-16, n2-standard-32, n2-standard-48, and n2-standard-64 instance types. In addition, the higher MTU of 8,896 requires the selection of VPC-1, VPC-2 and VPC-3 for the deployment. High write speed and an MTU of 8,896 are feature-dependent and cannot be disabled individually within a configured instance. For more information on VPC-1, VPC-2, and VPC-3, refer to Rules for VPC-1, VPC-2, and VPC-3.

b. Activate write once, read many (WORM) storage, if desired.

   WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

   Learn more about WORM storage.

c. If you activate WORM storage, select the retention period.

13. **Data Tiering in Google Cloud**: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then select a service account that has the predefined Storage Admin role.

    Note the following:

    - The Console sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Console agent service account as a user of the tiering service account, otherwise, you can't select it from the Console.
    - You can choose a specific volume tiering policy when you create or edit a volume.
    - If you disable data tiering, you can enable it on subsequent aggregates, but you'll need to turn off the system and add a service account from the Google Cloud Console.

      Learn more about data tiering.

14. **Create Volume**: Enter details for the new volume or click **Skip**.

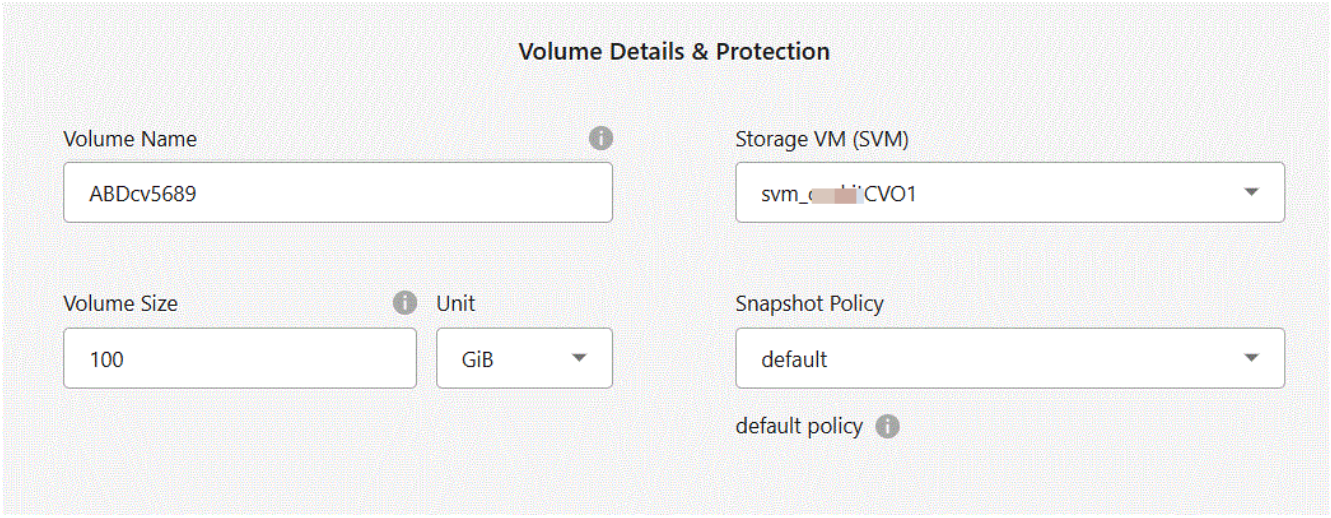
    Learn about supported client protocols and versions.

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

| Field | Description |
|---|---|
| Size | The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it. |
| Access control (for NFS only) | An export policy defines the clients in the subnet that can access the volume. By default, the Console enters a value that provides access to all instances in the subnet. |
| Permissions and Users / Groups (for CIFS only) | These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username. |

| Field | Description |
| --- | --- |
| Snapshot Policy | A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server. |
| Advanced options (for NFS only) | Select an NFS version for the volume: either NFSv3 or NFSv4. |
| Initiator group and IQN (for iSCSI only) | iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.<br><br>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.<br><br>iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs).<br><br>When you create an iSCSI volume, the Console automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts. |

The following image shows the first page of the volume creation wizard:




15. **CIFS Setup**: If you chose the CIFS protocol, set up a CIFS server.

| Field | Description |
| --- | --- |
| DNS Primary and Secondary IP Address | The IP addresses of the DNS servers that provide name resolution for the CIFS server.<br>The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.<br><br>If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address. |
| Active Directory Domain to join | The FQDN of the Active Directory (AD) domain that you want the CIFS server to join. |
| Credentials authorized to join the domain | The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain. |
| CIFS server NetBIOS name | A CIFS server name that is unique in the AD domain. |
| Organizational Unit | The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.<br><br>To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field.<br><br>Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD |
| DNS Domain | The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain. |
| NTP Server | Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. Refer to the NetApp Console automation docs for details.<br><br>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server. |

16. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and change the volume tiering policy, if needed.

    For more information, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

17. **Review & Approve**: Review and confirm your selections.
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the Google Cloud resources that the Console will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

**Result**

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the **Audit** page.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the system and click **Re-create environment**.

For additional help, go to NetApp Cloud Volumes ONTAP Support.

**After you finish**

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use ONTAP System Manager or the ONTAP CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

> After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Google Cloud portal, such as the system tags, and the labels set in the Google Cloud resources. Any changes made to these configurations may lead to unexpected behavior or data loss.

**Related links**

- Planning your Cloud Volumes ONTAP configuration in Google Cloud

# Google Cloud Platform Image Verification

## Learn how Google Cloud image is verfied in Cloud Volumes ONTAP

Google Cloud image verification complies with enhanced NetApp security requirements. Changes have been made to the script generating the images to sign the image along the way using private keys specifically generated for this task. You can verify the integrity of the Google Cloud image by using the signed digest and public certificate for Google Cloud which can be downloaded via NSS for a specific release.

> Google Cloud image verification is supported on Cloud Volumes ONTAP software version 9.13.0 or greater.

## Convert Google Cloud image to raw format for Cloud Volumes ONTAP

The image being used to deploy new instances, upgrades, or being used in existing images will be shared with the clients through the NetApp Support Site (NSS). The signed digest, and the certificates will be available to download through the NSS portal. Make sure you are downloading the digest and certificates for the right release corresponding to the image shared by NetApp Support. For instance, 9.13.0 images will have a 9.13.0 signed digest and certificates available on NSS.

**Why is this step needed?**

The images from Google Cloud cannot be downloaded directly. In order to verify the image against the signed digest and the certificates, you need to have a mechanism to compare the two files and download the image. To do so, you must export/convert the image into a disk.raw format and save the results in a storage bucket in Google Cloud. The disk.raw file is tarred and gzipped in the process.

The user/service-account will need privileges to perform the following:

- Access to Google storage bucket
- Write to Google Storage bucket
- Create cloud build jobs (used during export process)
- Access to the desired image
- Create export image tasks

To verify the image, it must be converted to a disk.raw format and then downloaded.

### Use Google Cloud command line to export Google Cloud image

The preferred way to export an image to Cloud Storage is to use the gcloud compute images export command. This command takes the provided image and converts it to a disk.raw file which gets tarred and gzipped. The generated file is saved at the destination URL and can then be downloaded for verification.

The user/account must have privileges to access and write to the desired bucket, export the image, and cloud builds (used by Google to export the image) to execute this operation.

### Export Google Cloud image using gcloud

**Click to display**

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

**Extract zipped files**

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

For more information on how to export an image through Google Cloud, refer to the Google Cloud doc on Exporting an image.

## Image signature verification

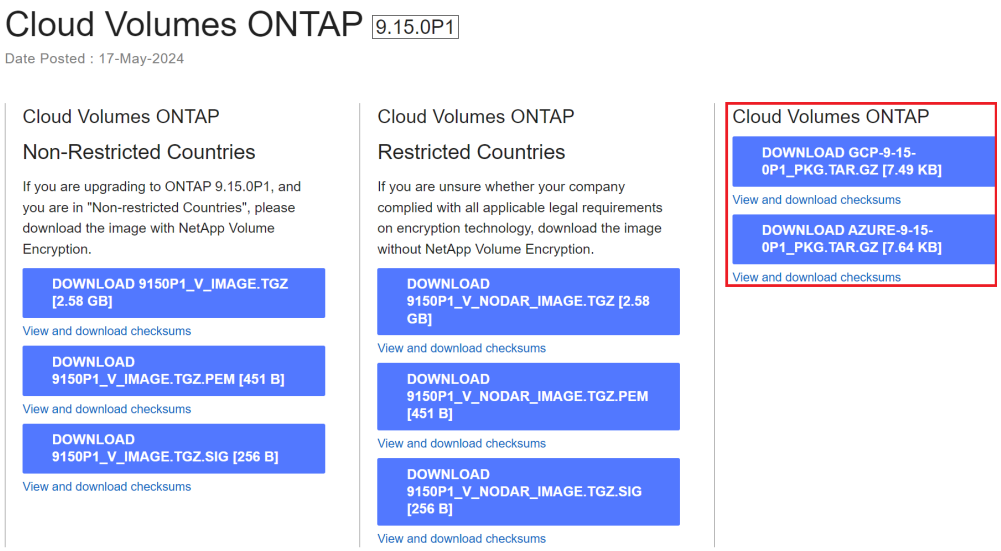
### Google Cloud image signature verification for Cloud Volumes ONTAP

To verify the exported Google Cloud signed image, you must download the image digest file from the NSS to validate the disk.raw file and digest file contents.

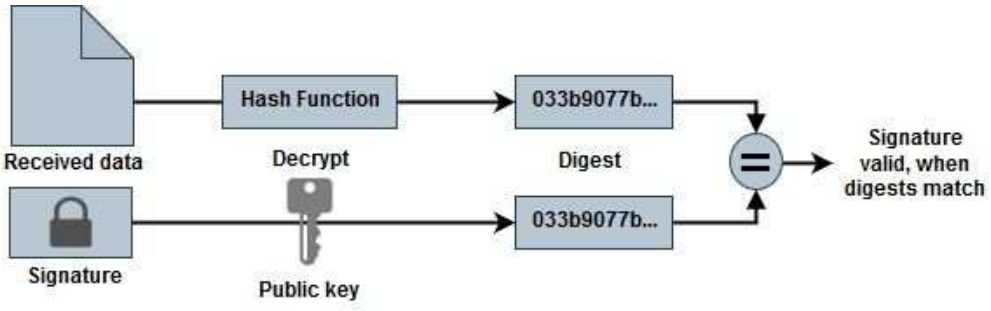
#### Signed image verification workflow summary

The following is an overview of the Google Cloud signed image verification workflow process.

- From the NSS, download the Google Cloud archive containing the following files:
  - Signed digest (.sig)
  - Certificate containing the public key (.pem)
  - Certificate chain (.pem)




- Download the converted disk.raw file
- Validate the certificate using the certificate chain
- Validate the signed digest using the certificate contain the public key
  - Decrypt the signed digest using the public key to extract the digest of the image file
  - Create a digest of the downloaded disk.raw file
  - Compare the two digest file for validation




### Verify the Google Cloud image disk.raw file for Cloud Volumes ONTAP using OpenSSL

You can verify the Google Cloud downloaded disk.raw file against the digest file contents available through the NSS using OpenSSL.

The OpenSSL commands to validate the image are compatible with Linux, macOS, and Windows machines.

#### Steps

1. Verify the certificate using OpenSSL.

**Click to display**

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
         e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
         22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
         38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
         fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
         bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Place the downloaded disk.raw file, the signature, and certificates in a directory.
3. Extract the public key from the certificate using OpenSSL.
4. Decrypt the signature using the extracted public key and verify the contents of the downloaded disk.raw file.

**Click to display**

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

## Copyright information



## Trademark information