



## **Get started in GCP**

### Cloud Manager

NetApp  
September 09, 2021

# Table of Contents

- Get started in GCP ..... 1
  - Getting started with Cloud Volumes ONTAP for Google Cloud ..... 1
  - Planning your Cloud Volumes ONTAP configuration in Google Cloud ..... 2
  - Networking requirements for Cloud Volumes ONTAP in GCP ..... 5
  - Create a service account for data tiering and backups ..... 17
  - Using customer-managed encryption keys with Cloud Volumes ONTAP ..... 20
  - Launching Cloud Volumes ONTAP in GCP ..... 21
  - Planning for VPC Service Controls in GCP ..... 32

# Get started in GCP

## Getting started with Cloud Volumes ONTAP for Google Cloud

Get started with Cloud Volumes ONTAP for GCP in a few steps.



### Create a Connector

If you don't have a [Connector](#) yet, an Account Admin needs to create one. [Learn how to create a Connector in GCP.](#)

When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to deploy a Connector if you don't have one yet.



### Plan your configuration

Cloud Manager 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.](#)



### Set up your networking

- a. Ensure that your VPC and subnets will support connectivity between the Connector 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 Connector service account.
- e. Enable outbound internet access from the target VPC so the Connector and Cloud Volumes ONTAP can contact several endpoints.

This step is important because the Connector can't manage Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for [the Connector and Cloud Volumes ONTAP](#).

[Learn more about networking requirements.](#)



### 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 [Cloud Backup Service](#) 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.](#)



#### Enable Google Cloud APIs

Enable the following [Google Cloud APIs in your project](#). These APIs are required to deploy the Connector 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



#### Launch Cloud Volumes ONTAP using Cloud Manager

Click **Add Working Environment**, 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

- [Evaluating](#)
- [Creating a Connector from Cloud Manager](#)
- [Installing the Connector software on a Linux host](#)
- [What Cloud Manager does with GCP permissions](#)

## Planning 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.

### Choosing a license type

Cloud Volumes ONTAP is available in two pricing options: pay-as-you-go and Bring Your Own License (BYOL). For pay-as-you-go, you can choose from three licenses: Explore, Standard, or Premium. Each license provides different capacity and compute options.

[Supported configurations for Cloud Volumes ONTAP 9.9.1 in GCP](#)

## Supported machine types

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

[Supported configurations for Cloud Volumes ONTAP 9.9.1 in GCP](#)

## Understanding 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 9.9.1 in GCP](#)

## Sizing your system in GCP

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](#)

### GCP disk type

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, see [Google Cloud documentation: Zonal Persistent disks \(Standard and SSD\)](#).

### GCP disk size

You need to choose an initial disk size when you deploy a Cloud Volumes ONTAP system. After that you can let Cloud Manager 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](#)

## GCP network information worksheet

When you deploy Cloud Volumes ONTAP in GCP, 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

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

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

| GCP 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

| GCP information  | Your value |
|------------------|------------|
| Region           |            |
| Zone             |            |
| VPC-0 and subnet |            |
| VPC-1 and subnet |            |

| GCP information                     | Your value |
|-------------------------------------|------------|
| VPC-2 and subnet                    |            |
| VPC-3 and subnet                    |            |
| Firewall policy (if using your own) |            |

## Choosing a write speed

Cloud Manager 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.](#)

## Choosing 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 Cloud Manager, 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.

# Networking requirements for Cloud Volumes ONTAP in GCP

Set up your Google Cloud Platform networking so Cloud Volumes ONTAP systems can operate properly. This includes networking for the Connector and Cloud Volumes ONTAP.

If you want to deploy an HA pair, you should [learn how HA pairs work in GCP.](#)

## Requirements for Cloud Volumes ONTAP

The following requirements must be met in GCP.

### Internal load balancers

Cloud Manager automatically creates three Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the Cloud Volumes ONTAP HA pair. (Prior to 9.9.0, four load balancers were created.) 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 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.

### **One or multiple zones for HA pairs**

You can ensure the high availability of your data by deploying an HA configuration across multiple or in a single zone. Cloud Manager will prompt 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.

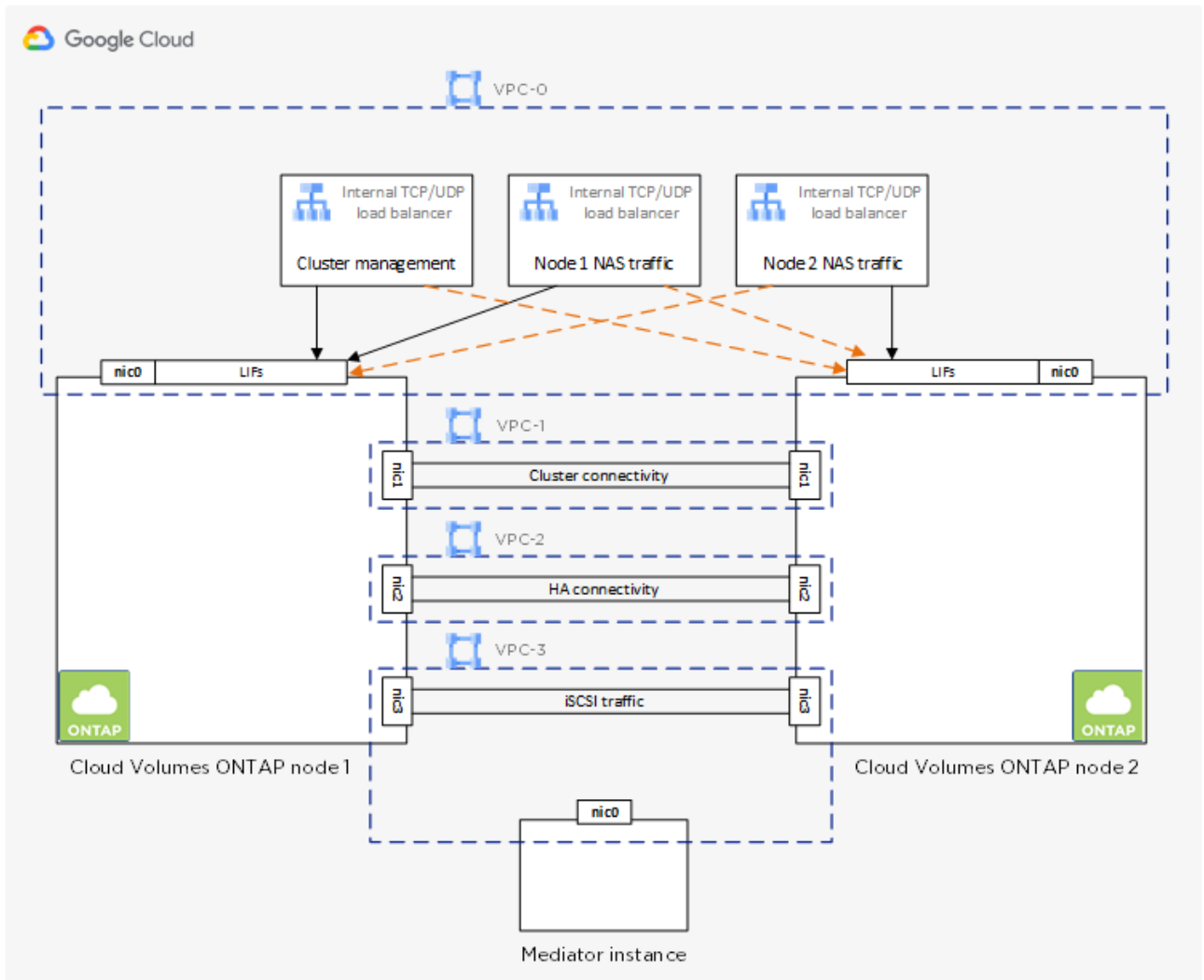
### **Four Virtual Private Clouds for HA pairs**

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

Cloud Manager will prompt 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 for HA pairs

A private subnet is required for each VPC.

If you place the Connector 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.

## One Virtual Private Cloud for single node systems

One VPC is required for a single node system.

## Shared VPCs

Cloud Volumes ONTAP and the Connector 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 Connector and Cloud Volumes ONTAP

virtual machine instances in a *service project*. [Google Cloud documentation: Shared VPC overview](#).

The only requirement when using a shared VPC is to provide the [Compute Network User role](#) to the Connector service account. Cloud Manager needs these permissions to query the firewalls, VPC, and subnets in the host project.

### Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow HTTP/HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

[Learn how to configure AutoSupport.](#)



If you're using an HA pair, the HA mediator doesn't require outbound internet access.

### Private IP addresses

Cloud Manager allocates the following number of private IP addresses to Cloud Volumes ONTAP in GCP:

- **Single node:** 3 or 4 private IP addresses

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.

- **HA pair:** 15 or 16 private IP addresses
  - 7 or 8 private IP addresses for VPC-0

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
```

- Two private IP addresses for VPC-1
- Two private IP addresses for VPC-2
- Three private IP addresses for VPC-3

### Firewall rules

You don't need to create firewall rules because Cloud Manager does that for you. If you need to use your own, refer to the firewall rules listed below.

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. [Learn more](#).

- 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](#).

### Connection from Cloud Volumes ONTAP to Google Cloud Storage for data tiering

If you want 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 (if you're using an HA pair, this is the subnet in VPC-0). For instructions, refer to [Google Cloud documentation: Configuring Private Google Access](#).

For additional steps required to set up data tiering in Cloud Manager, see [Tiering cold data to low-cost object storage](#).

### Connections to ONTAP systems in other networks

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

For instructions, refer to [Google Cloud documentation: Cloud VPN overview](#).

## Requirements for the Connector

Set up your networking so that the Connector can manage resources and processes within your public cloud environment. The most important step is ensuring outbound internet access to various endpoints.



If your network uses a proxy server for all communication to the internet, you can specify the proxy server from the Settings page. Refer to [Configuring the Connector to use a proxy server](#).

### Connection to target networks

A Connector requires a network connection to the VPCs in which you want to deploy Cloud Volumes ONTAP. If you're deploying an HA pair, then the Connector needs a connection to all four VPCs.

### Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment. A Connector contacts the following endpoints when managing resources in GCP:

| Endpoints  | Purpose  |
|--|--|
| <a href="https://www.googleapis.com">https://www.googleapis.com</a>  | Enables the Connector to contact Google APIs for deploying and managing Cloud Volumes ONTAP in GCP.        |
| <a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>  | API requests to NetApp Cloud Central.  |
| <a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>  | Provides access to software images, manifests, and templates.  |
| <a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a><br><a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a><br><a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a><br><a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a> | Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images. |

| Endpoints   | Purpose  |
|---|--|
| https://cloudmanagerinfraproduct.azurecr.io<br>*.blob.core.windows.net  | Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager. |
| https://kinesis.us-east-1.amazonaws.com   | Enables NetApp to stream data from audit records.  |
| https://cloudmanager.cloud.netapp.com   | Communication with the Cloud Manager service, which includes Cloud Central accounts.   |
| https://netapp-cloud-account.auth0.com  | Communication with NetApp Cloud Central for centralized user authentication.   |
| support.netapp.com:443<br>https://mysupport.netapp.com  | Communication with NetApp AutoSupport. Note that the Connector communicates with support.netapp.com:443, which redirects to https://mysupport.netapp.com.          |
| https://support.netapp.com/svcgw<br>https://support.netapp.com/ServiceGW/entitlement<br>https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com<br>https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com   | Communication with NetApp for system licensing and support registration.   |
| https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com<br>https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com<br>https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com   | Enables NetApp to collect information needed to troubleshoot support issues.   |
| https://ipa-signer.cloudmanager.netapp.com  | Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)  |
| <p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> <li>• https://repo1.maven.org/maven2</li> <li>• https://oss.sonatype.org/content/repositories</li> <li>• https://repo.typesafe.com</li> </ul> <p>Third-party locations are subject to change.</p> | During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.   |

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. The machine running the web browser must have connections to the following endpoints:

| Endpoints  | Purpose   |
|--|---|
| The Connector host   | <p>You must enter the host's IP address from a web browser to load the Cloud Manager console.</p> <p>Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host:</p> <ul style="list-style-type: none"> <li>• A private IP works if you have a VPN and direct connect access to your virtual network</li> <li>• A public IP works in any networking scenario</li> </ul> <p>In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets.</p> |
| <a href="https://auth0.com">https://auth0.com</a><br><a href="https://cdn.auth0.com">https://cdn.auth0.com</a><br><a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a><br><a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a> | Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.  |
| <a href="https://widget.intercom.io">https://widget.intercom.io</a>  | For in-product chat that enables you to talk to NetApp cloud experts.   |

## Firewall rules for Cloud Volumes ONTAP

Cloud Manager creates GCP 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 your to use 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.

### Inbound rules

The source for inbound rules in the predefined firewall is 0.0.0.0/0.

To create your own firewall, 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 [Google Cloud documentation: Load Balancer Firewall Rules](#).

| Protocol | Port | Purpose   |
|----------|------|---|
| All ICMP | All  | Pinging the instance  |
| HTTP     | 80   | HTTP access to the System Manager web console using the IP address of the cluster management LIF  |
| HTTPS    | 443  | HTTPS access to the 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               |

| Protocol | Port        | Purpose  |
|----------|-------------|--|
| 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  |
| 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 source is the interface (IP address) on 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  |
|------------|-------------|---------------------|--|----------------------------|--|
| Cluster    | All traffic | All traffic         | All LIFs on one node                         | All LIFs on the other node | Intercluster communications (Cloud Volumes ONTAP HA only)        |
|            | TCP         | 3000                | Node management LIF                          | HA mediator                | ZAPI calls (Cloud Volumes ONTAP HA only)                         |
|            | ICMP        | 1                   | Node management LIF                          | HA mediator                | Keep alive (Cloud Volumes ONTAP HA only)                         |
| 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         | 1860<br>0–18<br>699 | 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         | 1110<br>4           | Intercluster LIF                             | ONTAP intercluster LIFs    | Management of intercluster communication sessions for SnapMirror |
|            | TCP         | 1110<br>5           | Intercluster LIF                             | ONTAP intercluster LIFs    | SnapMirror data transfer   |
| Syslog     | UDP         | 514                 | Node management LIF                          | Syslog server              | Syslog forward messages  |

## Firewall rules for VPC-1, VPC-2, and VPC-3

In GCP, 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 policy that Cloud Manager creates for instances in VPC-1, VPC-2, and VPC-3 enables 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).

## Firewall rules for the Connector

The firewall rules for the Connector requires both inbound and outbound rules.

### Inbound rules

| Protocol | Port | Purpose  |
|----------|------|--|
| SSH      | 22   | Provides SSH access to the Connector host                                  |
| HTTP     | 80   | Provides HTTP access from client web browsers to the local user interface  |
| HTTPS    | 443  | Provides HTTPS access from client web browsers to the local user interface |

### Outbound rules

The predefined firewall rules for the Connector 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 firewall rules for the Connector includes the following outbound rules.

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

#### Advanced outbound rules

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



The source IP address is the Connector host.

| Service                   | Protocol | Port | Destination  | Purpose  |
|---------------------------|----------|------|--|--|
| Active Directory          | TCP      | 88   | Active Directory forest                            | Kerberos V authentication  |
|                           | TCP      | 139  | Active Directory forest                            | NetBIOS service session  |
|                           | TCP      | 389  | Active Directory forest                            | LDAP   |
|                           | TCP      | 445  | Active Directory forest                            | Microsoft SMB/CIFS over TCP with NetBIOS framing                       |
|                           | TCP      | 464  | Active Directory forest                            | Kerberos V change & set password (SET_CHANGE)                          |
|                           | TCP      | 749  | Active Directory forest                            | Active Directory Kerberos V change & set password (RPCSEC_GSS)         |
|                           | UDP      | 137  | Active Directory forest                            | NetBIOS name service   |
|                           | UDP      | 138  | Active Directory forest                            | NetBIOS datagram service   |
|                           | UDP      | 464  | Active Directory forest                            | Kerberos key administration  |
| API calls and AutoSupport | HTTPS    | 443  | Outbound internet and ONTAP cluster management LIF | API calls to GCP and ONTAP, and sending AutoSupport messages to NetApp |
| API calls                 | TCP      | 3000 | ONTAP cluster management LIF                       | API calls to ONTAP   |
| DNS                       | UDP      | 53   | DNS  | Used for DNS resolve by Cloud Manager                                  |

## Create a service account for data tiering and backups

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 [Cloud Backup Service](#) 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.

Create service account

✓ Service account details

2 Grant this service account access to project (optional)  
Grant this service account access to OCCM-Dev so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Select a role

Condition

storage admin

Cloud ML Service Agent  
Cloud ML service agent can act as log writer, Cloud Storage admin, Artifact Registry Reader, BigQuery writer, and service account access token creator.

Storage Admin  
Full control of GCS resources.

Storage HMAC Key Admin  
Full control of GCS HMAC Keys.

Storage Object Admin  
Full control of GCS objects.

MANAGE ROLES

3

DONE

- c. **Grant users access to this service account:** Add the Connector 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 the Cloud Backup Service.

Create service account

✓ Service account details

|

✓ Grant this service account access to project (optional)

|

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com ✕ ?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role ?

Grant users the permission to administer this service account

DONE

CANCEL

### What's next?

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

Details and Credentials

default-project

Google Cloud Project

gcp-sub2

Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account 

Service Account Name

account1

 Add Labels

Optional Field | Up to four labels

Credentials

User Name

admin

Password

Confirm Password

## 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 Cloud Manager API 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 Cloud Manager Connector service account has the correct permissions in the project where the key is stored.

The permissions are provided by the [Cloud Manager YAML file](#) 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.list
- 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 on the key.

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

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. Use the "GcpEncryption" parameter with your API request when creating a working environment.

### Example

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

Refer to the [Cloud Manager automation docs](#) for more details about using the "GcpEncryption" parameter.

## Launching Cloud Volumes ONTAP in GCP

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

### Before you get started

You need the following to create a working environment.

- A Connector that's up and running.
  - You should have a [Connector that is associated with your workspace](#).
  - [You should be prepared to leave the Connector running at all times](#).
  - The service account associated with the Connector [should have the latest permissions](#).
- An understanding of the configuration that you want to use.

You should have prepared by choosing a configuration and by obtaining GCP networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).

- An understanding of what's required to choose a specific licensing option in the Add Working Environment wizard.

| Licensing option | Requirement                             | How to meet the requirement  |
|------------------|---|--|
| PAYGO free trial | A Marketplace subscription is required. | You'll have the option to subscribe to your cloud provider's marketplace from the <b>Details &amp; Credentials</b> page. |

| Licensing option    | Requirement   | How to meet the requirement  |
|---------------------|---|--|
| Freemium            | A Marketplace subscription or NetApp Support Site (NSS) account is required.  | You'll have the option to subscribe to your cloud provider's marketplace from the <b>Details &amp; Credentials</b> page<br><br>You can enter your NSS account on the <b>Charging Methods and NSS Account</b> page. |
| Capacity-based BYOL | A Marketplace subscription or NetApp Support Site (NSS) account is required.<br><br>A Marketplace subscription is recommended for capacity-based charging in the event that your account doesn't have a valid capacity-based license, or in the event that your provisioned capacity exceeds the licensed capacity. | You'll have the option to subscribe to your cloud provider's marketplace from the <b>Details &amp; Credentials</b> page<br><br>You can enter your NSS account on the <b>Charging Methods and NSS Account</b> page. |
| Node-based BYOL     | The 20-digit serial number (license key) is required.   | You'll enter the serial number on the <b>Charging Methods and NSS Account</b> page.  |

- 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

## Launching a single-node system in GCP

Create a working environment in Cloud Manager to launch Cloud Volumes ONTAP in GCP.


### Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Google Cloud** and **Cloud Volumes ONTAP**.
3. If you're prompted, [create a Connector](#).
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  |
|--------------------------|--|
| Working Environment Name | Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the GCP VM instance. It also uses the name as the prefix for the predefined security group, if you select that option. |



| Field                  | Description   |
|------------------------|---|
| Service Account Name   | If you plan to use <a href="#">data tiering</a> or <a href="#">Cloud Backup</a> with Cloud Volumes ONTAP, then you need to enable <b>Service Account</b> and select a service account that has the predefined Storage Admin role. <a href="#">Learn how to create a service account.</a>  |
| Add Labels             | <p>Labels are metadata for your GCP resources. Cloud Manager adds the labels to the Cloud Volumes ONTAP system and GCP resources associated with the system.</p> <p>You can add up to four labels from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four labels when creating a working environment.</p> <p>For information about labels, refer to <a href="#">Google Cloud Documentation: Labeling Resources</a>.</p>  |
| User name and password | These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.   |
| Edit Project           | <p>Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where Cloud Manager resides.</p> <p>If you don't see any additional projects in the drop-down list, then you haven't yet associated the Cloud Manager 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 Cloud Manager role to that project. You'll need to repeat this step for each project.</p> <div>  <p>This is the service account that you set up for Cloud Manager, <a href="#">as described on this page</a>.</p> </div> <p>Click <b>Add Subscription</b> to associate the selected credentials with a subscription.</p> <p>To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a GCP project that's associated with a subscription to Cloud Volumes ONTAP from the GCP Marketplace.</p> |

The following video shows how to associate a pay-as-you-go Marketplace subscription to your GCP project:

► [https://docs.netapp.com/us-en/occm//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/us-en/occm//media/video_subscribing_gcp.mp4) (video)

- Services:** Select the services that you want to use on this system. In order to select Cloud Backup, or to use Tiering, you must have specified the Service Account in step 3.
- Location & Connectivity:** Select a location, choose a firewall policy, and select the checkbox to confirm network connectivity to Google Cloud storage for data tiering.

If you want 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](#).

7. **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 these charging methods.](#)
  - [Learn what's required in the wizard for the licensing method that you want to use.](#)
8. **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.

9. **Licensing:** Change the Cloud Volumes ONTAP version as needed, select a license, and select a virtual machine type.

If your needs change after you launch the system, you can modify the license or virtual machine type later.



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.6 RC1 and 9.6 GA is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

10. **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 Cloud Manager 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, see [Sizing your system in GCP](#).

11. **Write Speed & WORM:** Choose **Normal** or **High** write speed, and activate write once, read many (WORM) storage, if desired.

Choosing a write speed is supported with single node systems only.

[Learn more about write speed.](#)

WORM can't be enabled if Cloud Backup was enabled or if data tiering was enabled.

[Learn more about WORM storage.](#)

12. **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 GCP account (required for Cloud Volumes ONTAP 9.6).

Note the following:

- Cloud Manager 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 Connector

service account as a user of the tiering service account, otherwise, you can't select it from Cloud Manager.

- For help with adding a GCP account, see [Setting up and adding GCP 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 GCP console.

[Learn more about data tiering](#).

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

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, Cloud Manager 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.  |
| 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)       | <p>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</p> <p>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</p> <p>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).</p> <p>When you create an iSCSI volume, Cloud Manager 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, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p> |

The following image shows the Volume page filled out for the CIFS protocol:

Volume Details, Protection & Protocol

Details & Protection

Volume Name:

vol

Size (GB):

250

Snapshot Policy:

default

Default Policy

Protocol

NFS

CIFS

iSCSI

Share name:

vol\_share

Permissions:

Full Control

Users / Groups:

engineering

Valid users and groups separated by a semicolon

14. **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. |
| 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.   |
| 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 <b>Use Active Directory Domain</b> 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. See the <a href="#">Cloud Manager automation docs</a> for details.                   |

15. **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, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

16. **Review & Approve:** Review and confirm your selections.

a. Review details about the configuration.

- b. Click **More information** to review details about support and the GCP resources that Cloud Manager will purchase.
- c. Select the **I understand...** check boxes.
- d. Click **Go**.

## Result

Cloud Manager deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the working environment 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 System Manager or the CLI.

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

## Launching an HA pair in GCP


Create a working environment in Cloud Manager to launch Cloud Volumes ONTAP in GCP.

### Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Google Cloud** and **Cloud Volumes ONTAP HA**.
3. **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  |
|--------------------------|--|
| Working Environment Name | Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the GCP 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 <a href="#">Tiering</a> or <a href="#">Cloud Backup</a> services, you need to enable the <b>Service Account</b> switch and then select the Service Account that has the predefined Storage Admin role.  |
| Add Labels               | <p>Labels are metadata for your GCP resources. Cloud Manager adds the labels to the Cloud Volumes ONTAP system and GCP resources associated with the system.</p> <p>You can add up to four labels from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four labels when creating a working environment.</p> <p>For information about labels, refer to <a href="#">Google Cloud Documentation: Labeling Resources</a>.</p> |

| Field                  | Description  |
|------------------------|--|
| User name and password | These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.  |
| Edit Project           | <p>Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where Cloud Manager resides.</p> <p>If you don't see any additional projects in the drop-down list, then you haven't yet associated the Cloud Manager 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 Cloud Manager role to that project. You'll need to repeat this step for each project.</p> <div>  <p>This is the service account that you set up for Cloud Manager, <a href="#">as described in step 4b on this page</a>.</p> </div> <p>Click <b>Add Subscription</b> to associate the selected credentials with a subscription.</p> <p>To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a GCP project that's associated with a subscription to Cloud Volumes ONTAP from the GCP Marketplace.</p> |

The following video shows how to associate a pay-as-you-go Marketplace subscription to your GCP project:

► [https://docs.netapp.com/us-en/occm//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/us-en/occm//media/video_subscribing_gcp.mp4) (video)

- Services:** Select the services that you want to use on this system. In order to select Cloud Backup, or to use Tiering, you must have specified the Service Account in step 3.
- HA Deployment Models:** Choose multiple zones (recommended) or a single zone for the HA configuration. Then select a region and zones.

[Learn more about HA deployment models.](#)

- 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.](#)

- 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 these charging methods.](#)
  - [Learn what's required in the wizard for the licensing method that you want to use.](#)
- 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.

9. **Licensing:** Change the Cloud Volumes ONTAP version as needed, select a license, and select a virtual machine type.

If your needs change after you launch the system, you can modify the license or virtual machine type later.



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.8 RC1 and 9.8 GA is available. The update does not occur from one release to another—for example, from 9.7 to 9.8.

10. **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 Cloud Manager 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, see [Sizing your system in GCP](#).

11. **WORM:** Activate write once, read many (WORM) storage, if desired.

WORM can't be enabled if data tiering was enabled. [Learn more about WORM storage](#).

12. **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 select a service account that has the predefined Storage Admin role.

Note the following:

- Cloud Manager 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 Connector service account as a user of the tiering service account, otherwise, you can't select it from Cloud Manager.
- 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 GCP console.

[Learn more about data tiering](#).

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

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. |

| Field  | Description   |
|--|---|
| Access control (for NFS only)                  | An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager 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.  |
| 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)       | <p>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</p> <p>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</p> <p>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).</p> <p>When you create an iSCSI volume, Cloud Manager 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, <a href="#">use the IQN to connect to the LUN from your hosts</a>.</p> |

The following image shows the Volume page filled out for the CIFS protocol:

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

*Default Policy*

#### Protocol

NFS **CIFS** iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon



14. **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. |
| 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.   |
| 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 <b>Use Active Directory Domain</b> 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. See the <a href="#">Cloud Manager automation docs</a> for details.                   |

15. **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, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

16. **Review & Approve:** Review and confirm your selections.

- Review details about the configuration.
- Click **More information** to review details about support and the GCP resources that Cloud Manager will purchase.
- Select the **I understand...** check boxes.
- Click **Go**.

## Result

Cloud Manager deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the working environment 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 System Manager or the CLI.

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

## Planning for VPC Service Controls in GCP

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

NetApp services such as Cloud Central and Cloud Manager communicate 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 Cloud Manager Connector.

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

### Images

Both Cloud Volumes ONTAP and Cloud Manager use images from a project within GCP that is managed by NetApp. This can affect the deployment of the Cloud Manager Connector 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 Connector 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 Connector and Cloud Volumes ONTAP.

#### Deploying a Connector

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

#### Deploying Cloud Volumes ONTAP

- The Cloud Manager 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 [GCP VPC Service Controls Policy Documentation](#).

To set the policies that Cloud Manager 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 Connector and for Cloud Volumes ONTAP.

## Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.