



Get started

Cloud Volumes ONTAP

NetApp
September 22, 2022

Table of Contents

- Get started 1
 - Learn about Cloud Volumes ONTAP 1
 - Get started in Amazon Web Services 2
 - Get started in Microsoft Azure 67
 - Get started in Google Cloud 96

Get started

Learn about Cloud Volumes ONTAP

Cloud Volumes ONTAP enables you to optimize your cloud storage costs and performance while enhancing data protection, security, and compliance.

Cloud Volumes ONTAP is a software-only storage appliance that runs ONTAP data management software in the cloud. It provides enterprise-grade storage with the following key features:

- Storage efficiencies

Leverage built-in data deduplication, data compression, thin provisioning, and cloning to minimize storage costs.

- High availability

Ensure enterprise reliability and continuous operations in case of failures in your cloud environment.

- Data protection

Cloud Volumes ONTAP leverages SnapMirror, NetApp's industry-leading replication technology, to replicate on-premises data to the cloud so it's easy to have secondary copies available for multiple use cases.

Cloud Volumes ONTAP also integrates with Cloud Backup to deliver backup and restore capabilities for protection, and long-term archive of your cloud data.

[Learn more about Cloud Backup](#)

- Data tiering

Switch between high and low-performance storage pools on-demand without taking applications offline.

- Application consistency

Ensure consistency of NetApp Snapshot copies using NetApp SnapCenter.

[Learn more about SnapCenter](#)

- Data security

Cloud Volumes ONTAP supports data encryption and provides protection against viruses and ransomware.

- Privacy compliance controls

Integration with Cloud Data Sense helps you understand data context and identify sensitive data.

[Learn more about Cloud Data Sense](#)



Licenses for ONTAP features are included with Cloud Volumes ONTAP.

[View supported Cloud Volumes ONTAP configurations](#)

Get started in Amazon Web Services

Quick start for Cloud Volumes ONTAP in AWS

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

1

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 AWS](#).

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.

2

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](#).

3

Set up your networking

- a. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
- b. 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](#).

- c. Set up a VPC endpoint to the S3 service.

A VPC endpoint is required if you want to tier cold data from Cloud Volumes ONTAP to low-cost object storage.

[Learn more about networking requirements](#).

4

Set up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you need to ensure that an active Customer Master Key (CMK) exists. You also need to modify the key policy for each CMK by adding the IAM role that provides permissions to the Connector as a *key user*. [Learn more](#).

5

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

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

Plan your Cloud Volumes ONTAP configuration in AWS

When you deploy Cloud Volumes ONTAP in AWS, 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 AWS regions. [View the full list of supported regions](#).

Newer AWS regions must be enabled before you can create and manage resources in those regions. [Learn how to enable a region](#).

Choose a supported instance

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

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

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 AWS](#)

Size your system in AWS

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 an instance type, disk type, and disk size:

Instance type

- Match your workload requirements to the maximum throughput and IOPS for each EC2 instance type.

- If several users write to the system at the same time, choose an instance type that has enough CPUs to manage the requests.
- If you have an application that is mostly reads, then choose a system with enough RAM.
 - [AWS Documentation: Amazon EC2 Instance Types](#)
 - [AWS Documentation: Amazon EBS–Optimized Instances](#)

EBS disk type

At a high level, the differences between EBS disk types are as follows. To learn more about the use cases for EBS disks, refer to [AWS Documentation: EBS Volume Types](#).

- *General Purpose SSD (gp3)* disks are the lowest-cost SSDs that balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS and throughput. gp3 disks are supported with Cloud Volumes ONTAP 9.7 and later.

When you select a gp3 disk, Cloud Manager fills in default IOPS and throughput values that provide performance that is equivalent to a gp2 disk based on the selected disk size. You can increase the values to get better performance at a higher cost, but we do not support lower values because it can result in inferior performance. In short, stick with the default values or increase them. Don't lower them. [Learn more about gp3 disks and their performance](#).

Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with gp3 disks. [Learn more about Elastic Volumes support](#).

- *General Purpose SSD (gp2)* disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS.
- *Provisioned IOPS SSD (io1)* disks are for critical applications that require the highest performance at a higher cost.

Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with io1 disks. [Learn more about Elastic Volumes support](#).

- *Throughput Optimized HDD (st1)* disks are for frequently accessed workloads that require fast and consistent throughput at a lower price.



Tiering data to object storage is not recommended when using Throughput Optimized HDDs (st1).

EBS disk size

If you choose a configuration that doesn't support the [Amazon EBS Elastic Volumes feature](#), then you need to choose an initial disk size when you launch a Cloud Volumes ONTAP system. After that, you can [let Cloud Manager manage a system's capacity for you](#), but if you want to [create aggregates yourself](#), be aware of the following:

- All disks in an aggregate must be the same size.
- The performance of EBS disks is tied to disk size. The size determines the baseline IOPS and maximum burst duration for SSD disks and the baseline and burst throughput for HDD disks.
- Ultimately, you should choose the disk size that gives you the *sustained performance* that you need.
- Even if you do choose larger disks (for example, six 4 TiB disks), you might not get all of the IOPS because the EC2 instance can reach its bandwidth limit.

For more details about EBS disk performance, refer to [AWS Documentation: EBS Volume Types](#).

As noted above, choosing a disk size is not supported with Cloud Volumes ONTAP configurations that support the Amazon EBS Elastic Volumes feature. [Learn more about Elastic Volumes support](#).

Watch the following video for more details about sizing your Cloud Volumes ONTAP system in AWS:



View default system disks

In addition to the storage for user data, Cloud Manager 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 AWS.](#)



The Connector also requires a system disk. [View details about the Connector's default configuration.](#)

Prepare to deploy Cloud Volumes ONTAP in an AWS Outpost

If you have an AWS Outpost, you can deploy Cloud Volumes ONTAP in that Outpost by selecting the Outpost VPC in the Working Environment wizard. The experience is the same as any other VPC that resides in AWS. Note that you will need to first deploy a Connector in your AWS Outpost.

There are a few limitations to point out:

- Only single node Cloud Volumes ONTAP systems are supported at this time
- The EC2 instances that you can use with Cloud Volumes ONTAP are limited to what's available in your Outpost

- Only General Purpose SSDs (gp2) are supported at this time

Collect networking information

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

Single node or HA pair in a single AZ

| AWS information | Your value |
|------------------------------------|------------|
| Region | |
| VPC | |
| Subnet | |
| Security group (if using your own) | |

HA pair in multiple AZs

| AWS information | Your value |
|---|------------|
| Region | |
| VPC | |
| Security group (if using your own) | |
| Node 1 availability zone | |
| Node 1 subnet | |
| Node 2 availability zone | |
| Node 2 subnet | |
| Mediator availability zone | |
| Mediator subnet | |
| Key pair for the mediator | |
| Floating IP address for cluster management port | |
| Floating IP address for data on node 1 | |
| Floating IP address for data on node 2 | |
| Route tables for floating IP addresses | |

Choose a write speed

Cloud Manager enables you to choose a write speed setting for Cloud Volumes ONTAP. 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 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.

Set up your networking

Networking requirements for Cloud Volumes ONTAP in AWS

Cloud Manager 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.

General requirements

The following requirements must be met in AWS.

Outbound internet access for Cloud Volumes ONTAP nodes

Cloud Volumes ONTAP nodes require outbound internet access for NetApp AutoSupport, which proactively monitors the health of your system and sends messages to NetApp technical support.

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>

If you have a NAT instance, you must define an inbound security group rule that allows HTTPS traffic from the private subnet to the internet.

If an outbound internet connection isn't available to send AutoSupport messages, Cloud Manager automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server. The

only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you defined strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

After you've verified that outbound internet access is available, you can test AutoSupport to ensure that it can send messages. For instructions, refer to [ONTAP docs: Set up AutoSupport](#).

If Cloud Manager notifies you that AutoSupport messages can't be sent, [troubleshoot your AutoSupport configuration](#).

Outbound internet access for the HA mediator

The HA mediator instance must have an outbound connection to the AWS EC2 service so it can assist with storage failover. To provide the connection, you can add a public IP address, specify a proxy server, or use a manual option.

The manual option can be a NAT gateway or an interface VPC endpoint from the target subnet to the AWS EC2 service. For details about VPC endpoints, refer to [AWS Documentation: Interface VPC Endpoints \(AWS PrivateLink\)](#).

Private IP addresses

Cloud Manager automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP. You need to ensure that your networking has enough private IP addresses available.

The number of LIFs that Cloud Manager allocates 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.

IP addresses for a single node system

Cloud Manager allocates 6 IP addresses to a single node system:

- Cluster management LIF
- Node management LIF
- Intercluster LIF
- NAS data LIF
- iSCSI data LIF
- Storage VM management LIF

A storage VM management LIF is used with management tools like SnapCenter.

IP addresses for HA pairs

HA pairs require more IP addresses than a single node system does. These IP addresses are spread across different ethernet interfaces, as shown in the following image:



The number of private IP addresses required for an HA pair depends on which deployment model you choose. An HA pair deployed in a *single* AWS Availability Zone (AZ) requires 15 private IP addresses, while an HA pair deployed in *multiple* AZs requires 13 private IP addresses.

The following tables provide details about the LIFs that are associated with each private IP address.

LIFs for HA pairs in a single AZ

| LIF | Interface | Node | Purpose |
|--------------------|-----------|-------------------|--|
| Cluster management | eth0 | node 1 | Administrative management of the entire cluster (HA pair). |
| Node management | eth0 | node 1 and node 2 | Administrative management of a node. |
| Intercluster | eth0 | node 1 and node 2 | Cross-cluster communication, backup, and replication. |
| NAS data | eth0 | node 1 | Client access over NAS protocols. |

| LIF | Interface | Node | Purpose |
|----------------------|-----------|-------------------|---|
| iSCSI data | eth0 | node 1 and node 2 | Client access over the iSCSI protocol and system use for important networking workflows. These LIFs are required and should not be deleted. |
| Cluster connectivity | eth1 | node 1 and node 2 | Enables the nodes to communicate with each other and to move data within the cluster. |
| HA connectivity | eth2 | node 1 and node 2 | Communication between the two nodes in case of failover. |
| RSM iSCSI traffic | eth3 | node 1 and node 2 | RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator. |
| Mediator | eth0 | Mediator | A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes. |

LIFs for HA pairs in multiple AZs

| LIF | Interface | Node | Purpose |
|----------------------|-----------|-------------------|---|
| Node management | eth0 | node 1 and node 2 | Administrative management of a node. |
| Intercluster | eth0 | node 1 and node 2 | Cross-cluster communication, backup, and replication. |
| iSCSI data | eth0 | node 1 and node 2 | Client access over the iSCSI protocol. This LIF also manages the migration of floating IP addresses between nodes. |
| Cluster connectivity | eth1 | node 1 and node 2 | Enables the nodes to communicate with each other and to move data within the cluster. |
| HA connectivity | eth2 | node 1 and node 2 | Communication between the two nodes in case of failover. |
| RSM iSCSI traffic | eth3 | node 1 and node 2 | RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator. |
| Mediator | eth0 | Mediator | A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes. |



When deployed in multiple Availability Zones, several LIFs are associated with [floating IP addresses](#), which don't count against the AWS private IP limit.

Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to [Security group rules](#).

Connection for data tiering

If you want to use EBS as a performance tier and AWS S3 as a capacity tier, you must ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Volumes ONTAP instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Volumes ONTAP cannot connect to the S3 service.

If you experience any issues, see [AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?](#)

Connections to ONTAP systems

To replicate data between a Cloud Volumes ONTAP system in AWS and ONTAP systems in other networks, you must have a VPN connection between the AWS VPC and the other network—for example, your corporate network. For instructions, see [AWS Documentation: Setting Up an AWS VPN Connection](#).

DNS and Active Directory for CIFS

If you want to provision CIFS storage, you must set up DNS and Active Directory in AWS or extend your on-premises setup to AWS.

The DNS server must provide name resolution services for the Active Directory environment. You can configure DHCP option sets to use the default EC2 DNS server, which must not be the DNS server used by the Active Directory environment.

For instructions, refer to [AWS Documentation: Active Directory Domain Services on the AWS Cloud: Quick Start Reference Deployment](#).

VPC sharing

Starting with the 9.11.1 release, Cloud Volumes ONTAP HA pairs are supported in AWS with VPC sharing. VPC sharing enables your organization to share subnets with other AWS accounts. To use this configuration, you must set up your AWS environment and then deploy the HA pair using the API.

[Learn how to deploy an HA pair in a shared subnet.](#)

Requirements for HA pairs in multiple AZs

Additional AWS networking requirements apply to Cloud Volumes ONTAP HA configurations that use multiple Availability Zones (AZs). You should review these requirements before you launch an HA pair because you must enter the networking details in Cloud Manager when you create the working environment.

To understand how HA pairs work, see [High-availability pairs](#).

Availability Zones

This HA deployment model uses multiple AZs to ensure high availability of your data. You should use a dedicated AZ for each Cloud Volumes ONTAP instance and the mediator instance, which provides a communication channel between the HA pair.

A subnet should be available in each Availability Zone.

Floating IP addresses for NAS data and cluster/SVM management

HA configurations in multiple AZs use floating IP addresses that migrate between nodes if failures occur. They are not natively accessible from outside the VPC, unless you [set up an AWS transit gateway](#).

One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. A fourth floating IP address for SVM management is optional.



A floating IP address is required for the SVM management LIF if you use SnapDrive for Windows or SnapCenter with the HA pair.

You need to enter the floating IP addresses in Cloud Manager when you create a Cloud Volumes ONTAP HA working environment. Cloud Manager allocates the IP addresses to the HA pair when it launches the system.

The floating IP addresses must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. Think of the floating IP addresses as a logical subnet that's outside of the VPCs in your region.

The following example shows the relationship between floating IP addresses and the VPCs in an AWS region. While the floating IP addresses are outside the CIDR blocks for all VPCs, they're routable to subnets through route tables.

AWS region



Cloud Manager automatically creates static IP addresses for iSCSI access and for NAS access from clients outside the VPC. You don't need to meet any requirements for these types of IP addresses.

Transit gateway to enable floating IP access from outside the VPC

If needed, [set up an AWS transit gateway](#) to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

Route tables

After you specify the floating IP addresses in Cloud Manager, you are then prompted to select the route tables that should include routes to the floating IP addresses. This enables client access to the HA pair.

If you have just one route table for the subnets in your VPC (the main route table), then Cloud Manager automatically adds the floating IP addresses to that route table. If you have more than one route table, it's very important to select the correct route tables when launching the HA pair. Otherwise, some clients might not have access to Cloud Volumes ONTAP.

For example, you might have two subnets that are associated with different route tables. If you select route table A, but not route table B, then clients in the subnet associated with route table A can access the HA

pair, but clients in the subnet associated with route table B can't.

For more information about route tables, refer to [AWS Documentation: Route Tables](#).

Connection to NetApp management tools

To use NetApp management tools with HA configurations that are in multiple AZs, you have two connection options:

1. Deploy the NetApp management tools in a different VPC and [set up an AWS transit gateway](#). The gateway enables access to the floating IP address for the cluster management interface from outside the VPC.
2. Deploy the NetApp management tools in the same VPC with a similar routing configuration as NAS clients.

Example HA configuration

The following image illustrates the networking components specific to an HA pair in multiple AZs: three Availability Zones, three subnets, floating IP addresses, and a route table.



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 and VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the VPC or VNet in which you launch Cloud Volumes ONTAP.

Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment.

| Endpoints | Purpose |
|---|---|
| https://support.netapp.com | To obtain licensing information and to send AutoSupport messages to NetApp support. |
| https://*.cloudmanager.cloud.netapp.com | To provide SaaS features and services within Cloud Manager. |
| https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net | To upgrade the Connector and its Docker components. |

Setting up an AWS transit gateway for HA pairs in multiple AZs

Set up an AWS transit gateway to enable access to an HA pair's [floating IP addresses](#) from outside the VPC where the HA pair resides.

When a Cloud Volumes ONTAP HA configuration is spread across multiple AWS Availability Zones, floating IP addresses are required for NAS data access from within the VPC. These floating IP addresses can migrate between nodes when failures occur, but they are not natively accessible from outside the VPC. Separate private IP addresses provide data access from outside the VPC, but they don't provide automatic failover.

Floating IP addresses are also required for the cluster management interface and the optional SVM management LIF.

If you set up an AWS transit gateway, you enable access to the floating IP addresses from outside the VPC where the HA pair resides. That means NAS clients and NetApp management tools outside the VPC can access the floating IPs.

Here's an example that shows two VPCs connected by a transit gateway. An HA system resides in one VPC, while a client resides in the other. You could then mount a NAS volume on the client using the floating IP address.



The following steps illustrate how to set up a similar configuration.

Steps

1. [Create a transit gateway and attach the VPCs to the gateway.](#)
2. Associate the VPCs with the transit gateway route table.
 - a. In the **VPC** service, click **Transit Gateway Route Tables**.
 - b. Select the route table.
 - c. Click **Associations** and then select **Create association**.
 - d. Choose the attachments (the VPCs) to associate and then click **Create association**.
3. Create routes in the transit gateway's route table by specifying the HA pair's floating IP addresses.

You can find the floating IP addresses on the Working Environment Information page in Cloud Manager. Here's an example:

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

The following sample image shows the route table for the transit gateway. It includes routes to the CIDR blocks of the two VPCs and four floating IP addresses used by Cloud Volumes ONTAP.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aedd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

| <input type="checkbox"/> | CIDR | Attachment | Resource type | Route type | Route state |
|--------------------------|---------------|--|---------------|------------|-------------|
| <input type="checkbox"/> | 10.100.0.0/16 | tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1 | VPC2 | propagated | active |
| <input type="checkbox"/> | 10.160.0.0/20 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC1 | propagated | active |
| <input type="checkbox"/> | 172.23.0.1/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC | static | active |
| <input type="checkbox"/> | 172.23.0.2/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Floating IP | static | active |
| <input type="checkbox"/> | 172.23.0.3/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Floating IP | static | active |
| <input type="checkbox"/> | 172.23.0.4/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Floating IP | static | active |

4. Modify the route table of VPCs that need to access the floating IP addresses.
 - a. Add route entries to the floating IP addresses.
 - b. Add a route entry to the CIDR block of the VPC where the HA pair resides.

The following sample image shows the route table for VPC 2, which includes routes to VPC 1 and the floating IP addresses.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

| Destination | Target | Status | Propagated |
|---------------|-----------------------|--------|------------|
| 10.100.0.0/16 | local | active | No |
| 0.0.0.0/0 | igw-07250bd01781e67df | active | No |
| 10.160.0.0/20 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.1/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.2/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.3/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.4/32 | tgw-015b7c249661ac279 | active | No |

VPC1

Floating IP Addresses

- Modify the route table for the HA pair's VPC by adding a route to the VPC that needs access to the floating IP addresses.

This step is important because it completes the routing between the VPCs.

The following sample image shows the route table for VPC 1. It includes a route to the floating IP addresses and to VPC 2, which is where a client resides. Cloud Manager automatically added the floating IPs to the route table when it deployed the HA pair.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

| Destination | Target | Status |
|---|-----------------------|--------|
| 10.160.0.0/20 | local | active |
| pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22) | vpce-cb51a0a2 | active |
| 0.0.0.0/0 | igw-b2182dd7 | active |
| 10.60.29.0/25 | pcx-589c3331 | active |
| 10.100.0.0/16 | tgw-015b7c249661ac279 | active |
| 10.129.0.0/20 | pcx-ff7e1396 | active |
| 172.23.0.1/32 | eni-0854d4715559c3cdb | active |
| 172.23.0.2/32 | eni-0854d4715559c3cdb | active |
| 172.23.0.3/32 | eni-0f76681216c3108ed | active |
| 172.23.0.4/32 | eni-0854d4715559c3cdb | active |

VPC2

Floating IP Addresses

- Mount volumes to clients using the floating IP address.

You can find the correct IP address in Cloud Manager by selecting a volume and clicking **Mount Command**.

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



7. If you're mounting an NFS volume, configure the export policy to match the subnet of the client VPC.

[Learn how to edit a volume.](#)

Related links

- [High-availability pairs in AWS](#)
- [Networking requirements for Cloud Volumes ONTAP in AWS](#)

Deploy an HA pair in a shared subnet

Starting with the 9.11.1 release, Cloud Volumes ONTAP HA pairs are supported in AWS with VPC sharing. VPC sharing enables your organization to share subnets with other AWS accounts. To use this configuration, you must set up your AWS environment and then deploy the HA pair using the API.

With [VPC sharing](#), a Cloud Volumes ONTAP HA configuration is spread across two accounts:

- The VPC owner account, which owns the networking (the VPC, subnets, route tables, and Cloud Volumes ONTAP security group)
- The participant account, where the EC2 instances are deployed in shared subnets (this includes the two HA nodes and the mediator)

In the case of a Cloud Volumes ONTAP HA configuration that is deployed across multiple Availability Zones, the HA mediator needs specific permissions to write to the route tables in the VPC owner account. You need to provide those permissions by setting up an IAM role that the mediator can assume.

The following image shows the components involved this deployment:



As described in the steps below, you'll need to share the subnets with the participant account, and then create the IAM role and security group in the VPC owner account.

When you create the Cloud Volumes ONTAP working environment, Cloud Manager automatically creates and attaches an IAM role to the mediator. This role assumes the IAM role that you created in the VPC owner account in order to make changes to the route tables associated with the HA pair.

Steps

1. Share the subnets in the VPC owner account with the participant account.

This step is required to deploy the HA pair in shared subnets.

[AWS documentation: Share a subnet](#)

2. In the VPC owner account, create a security group for Cloud Volumes ONTAP.

[Refer to the security group rules for Cloud Volumes ONTAP](#). Note that you don't need to create a security group for the HA mediator. Cloud Manager does that for you.

3. In the VPC owner account, create an IAM role that includes the following permissions:

```
"Action": [
    "ec2:AssignPrivateIpAddresses",
    "ec2:CreateRoute",
    "ec2>DeleteRoute",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcs",
    "ec2:ReplaceRoute",
    "ec2:UnassignPrivateIpAddresses"
```

4. Use the Cloud Manager API to create a new Cloud Volumes ONTAP working environment.

Note that you must specify the following fields:

- "securityGroupId"

The "securityGroupId" field should specify the security group that you created in the VPC owner account (see step 2 above).

- "assumeRoleArn" in the "haParams" object

The "assumeRoleArn" field should include the ARN of the IAM role that you created in the VPC owner account (see step 3 above).

For example:

```
"haParams": {
  "assumeRoleArn":
    "arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

[Learn about the Cloud Volumes ONTAP API](#)

Security group rules for AWS

Cloud Manager creates AWS security groups that include the inbound and outbound rules that the Connector and Cloud Volumes ONTAP need to operate successfully. You might want to refer to the ports for testing purposes or if you prefer your to use own security groups.

Rules for Cloud Volumes ONTAP

The security group for Cloud Volumes ONTAP requires both inbound and outbound rules.

Inbound rules

When you create a working environment and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VPC only:** the source 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 Connector resides. This is the recommended option.
- **All VPCs:** the source for inbound traffic is the 0.0.0.0/0 IP range.

| 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 | Connectivity with the Connector and 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 |
| 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 |
| 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 |

| Protocol | Port | Purpose |
|----------|------|--------------------------------|
| 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 |
|--------------|-------------|-------------|--|-------------------------------------|--|
| AutoSupport | HTTPS | 443 | Node management LIF | support.netapp.com | AutoSupport (HTTPS is the default) |
| | HTTP | 80 | Node management LIF | support.netapp.com | AutoSupport (only if the transport protocol is changed from HTTPS to HTTP) |
| | TCP | 3128 | Node management LIF | Connector | Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available |
| Backup to S3 | TCP | 5010 | Intercluster LIF | Backup endpoint or restore endpoint | Back up and restore operations for the Backup to S3 feature |
| 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 | 1860-18699 | 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 |

| Service | Protocol | Port | Source | Destination | Purpose |
|---------|----------|------|---------------------|---------------|-------------------------|
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |

Rules for the HA mediator external security group

The predefined external security group for the Cloud Volumes ONTAP HA mediator includes the following inbound and outbound rules.

Inbound rules

The source for inbound rules is 0.0.0.0/0.

| Protocol | Port | Purpose |
|----------|------|---------------------------------------|
| SSH | 22 | SSH connections to the HA mediator |
| TCP | 3000 | RESTful API access from the Connector |

Outbound rules

The predefined security group for the HA mediator 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 the HA mediator 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 HA mediator.

| Protocol | Port | Destination | Purpose |
|----------|------|----------------------|------------------------------------|
| HTTP | 80 | Connector IP address | Download upgrades for the mediator |
| HTTPS | 443 | AWS API services | Assist with storage failover |
| UDP | 53 | AWS API services | Assist with storage failover |



Rather than open ports 443 and 53, you can create an interface VPC endpoint from the target subnet to the AWS EC2 service.

Rules for the HA configuration internal security group

The predefined internal security group for a Cloud Volumes ONTAP HA configuration includes the following rules. This security group enables communication between the HA nodes and between the mediator and the nodes.

Cloud Manager always creates this security group. You do not have the option to use your own.

Inbound rules

The predefined security group includes the following inbound rules.

| Protocol | Port | Purpose |
|-------------|------|--|
| All traffic | All | Communication between the HA mediator and HA nodes |

Outbound rules

The predefined security group includes the following outbound rules.

| Protocol | Port | Purpose |
|-------------|------|--|
| All traffic | All | Communication between the HA mediator and HA nodes |

Rules for the Connector

The security group 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 and connections from Cloud Data Sense |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the local user interface |
| TCP | 3128 | Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deploying the Connector. |

Outbound rules

The predefined security group 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 security group for the Connector includes the following outbound rules.

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

| Protocol | Port | Purpose |
|----------|------|----------------------|
| 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 |
|---------------------------|----------|------|--|--|
| API calls and AutoSupport | HTTP | 443 | Outbound internet and ONTAP cluster management LIF | API calls to AWS and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |
| API calls | TCP | 3000 | ONTAP HA mediator | Communication with the ONTAP HA mediator |
| | TCP | 8088 | Backup to S3 | API calls to Backup to S3 |
| DNS | UDP | 53 | DNS | Used for DNS resolve by Cloud Manager |
| Cloud Data Sense | HTTP | 80 | Cloud Data Sense instance | Cloud Data Sense for Cloud Volumes ONTAP |

Setting up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you need to set up the AWS Key Management Service (KMS).

Steps

1. Ensure that an active Customer Master Key (CMK) exists.

The CMK can be an AWS-managed CMK or a customer-managed CMK. It can be in the same AWS account as Cloud Manager and Cloud Volumes ONTAP or in a different AWS account.

[AWS Documentation: Customer Master Keys \(CMKs\)](#)

2. Modify the key policy for each CMK by adding the IAM role that provides permissions to Cloud Manager as a *key user*.

Adding the IAM role as a key user gives Cloud Manager permissions to use the CMK with Cloud Volumes ONTAP.

[AWS Documentation: Editing Keys](#)

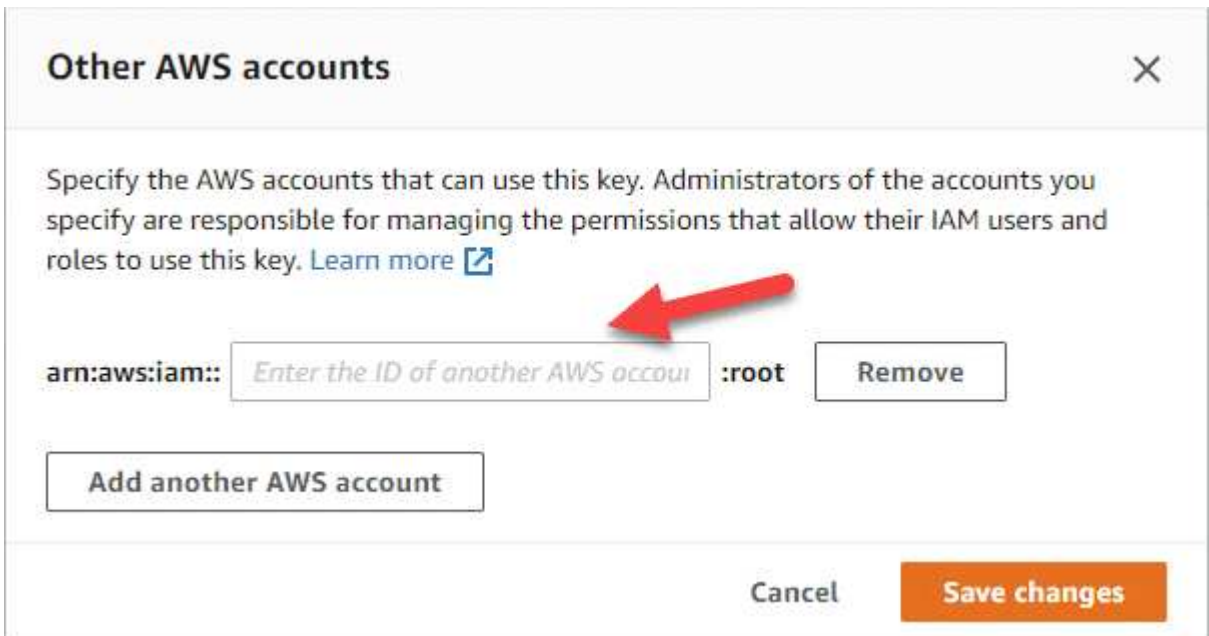
3. If the CMK is in a different AWS account, complete the following steps:
 - a. Go to the KMS console from the account where the CMK resides.
 - b. Select the key.

- c. In the **General configuration** pane, copy the ARN of the key.

You'll need to provide the ARN to Cloud Manager when you create the Cloud Volumes ONTAP system.

- d. In the **Other AWS accounts** pane, add the AWS account that provides Cloud Manager with permissions.

In most cases, this is the account where Cloud Manager resides. If Cloud Manager wasn't installed in AWS, it would be the account for which you provided AWS access keys to Cloud Manager.



- e. Now switch to the AWS account that provides Cloud Manager with permissions and open the IAM console.
- f. Create an IAM policy that includes the permissions listed below.
- g. Attach the policy to the IAM role or IAM user that provides permissions to Cloud Manager.

The following policy provides the permissions that Cloud Manager needs to use the CMK from the external AWS account. Be sure to modify the region and account ID in the "Resource" sections.


```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

For additional details about this process, see [AWS Documentation: Allowing users in other accounts to use a KMS key](#).

4. If you are using a customer-managed CMK, modify the key policy for the CMK by adding the Cloud Volumes ONTAP IAM role as a *key user*.

This step is required if you enabled data tiering on Cloud Volumes ONTAP and want to encrypt the data

stored in the S3 bucket.

You'll need to perform this step *after* you deploy Cloud Volumes ONTAP because the IAM role is created when you create a working environment. (Of course, you do have the option to use an existing Cloud Volumes ONTAP IAM role, so it's possible to perform this step before.)

[AWS Documentation: Editing Keys](#)

Set up IAM roles for Cloud Volumes ONTAP

An IAM role with the required permissions must be attached to each Cloud Volumes ONTAP node. The same is true for the HA mediator. It's easiest to let Cloud Manager create the IAM roles for you, but you can use your own roles.

This task is optional. When you create a Cloud Volumes ONTAP working environment, the default option is to let Cloud Manager create the IAM roles for you. If your business's security policies require you to create the IAM role yourself, then follow the steps below.



Providing your own IAM role is required in the AWS Commercial Cloud Services Environment. [Learn how to deploy Cloud Volumes ONTAP in C2S.](#)

Steps

1. Go to the AWS IAM console.
2. Create an IAM policy that includes the following permissions:
 - Cloud Volumes ONTAP nodes

Standard regions

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }
]
```

GovCloud (US) regions

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-us-gov:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

C2S environment

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

- HA mediator

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }]
}

```

3. Create an IAM role and attach the policy that you created in the previous step to the role.

Result

You now have IAM roles that you can select when you create a new Cloud Volumes ONTAP working environment.

More information

- [AWS documentation: Creating IAM policies](#)
- [AWS documentation: Creating IAM roles](#)

Set up licensing for Cloud Volumes ONTAP in AWS

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 working environment.

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. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 AWS 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](#).

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ **Pay-Per-TiB - Annual Contract**
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ **Pay-as-you-go**
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

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

Select Charging Method

| | | |
|---|-------------|---|
| <input type="radio"/> Professional | By capacity | ▼ |
| <input type="radio"/> Essential | By capacity | ▼ |
| <input checked="" type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node | By node | ▼ |

[View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.](#)

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 package or the Professional package.

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

- A license (BYOL) purchased from NetApp
- An hourly, pay-as-you-go (PAYGO) subscription from the AWS Marketplace
- An annual contract from the AWS Marketplace

[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.

Steps

1. [Contact NetApp Sales to obtain a license](#)
2. [Add your NetApp Support Site account to Cloud Manager](#)

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

Your license must be available from the Digital Wallet before you can use it with Cloud Volumes ONTAP. If needed, you can [manually add the license to the Digital Wallet](#).

3. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 AWS 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.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ **Pay-Per-TiB - Annual Contract**
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ **Pay-as-you-go**
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

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

Select Charging Method

| | | |
|--|-------------|---|
| <input checked="" type="radio"/> Professional | By capacity | ▼ |
| <input type="radio"/> Essential | By capacity | ▼ |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node | By node | ▼ |

[View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.](#)

PAYGO subscription

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

When you create a Cloud Volumes ONTAP working environment, Cloud Manager prompts you to subscribe to the agreement that's available in the AWS Marketplace. That subscription is then associated with the working environment for charging. You can use that same subscription for additional working environments.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 AWS Marketplace.

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". Below the title is a horizontal line. The main text reads: "Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe." Below this text are two selectable options, each in a light gray box. The first option is "Pay-Per-TiB - Annual Contract" with an unselected radio button; its description is "Pay for Cloud Volumes ONTAP with an annual, upfront payment." The second option is "Pay-as-you-go" with a selected radio button; its description is "Pay for Cloud Volumes ONTAP at an hourly rate." Below these options is another horizontal line, followed by the heading "The next steps:". There are two numbered steps: Step 1, "AWS Marketplace", with the instruction "Subscribe and then click **Set Up Your Account** to configure your account." Step 2, "Cloud Manager", with the instruction "Save your subscription and associate the Marketplace subscription with your AWS credentials." At the bottom right of the dialog are two buttons: a blue "Continue" button and a gray "Cancel" button.

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

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

[View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.](#)



You can manage the AWS Marketplace subscriptions associated with your AWS accounts from the Settings > Credentials page. [Learn how to manage your AWS accounts and subscriptions](#)

Annual contract

Pay annually by purchasing an annual contract from your cloud provider's marketplace.

Similar to an hourly subscription, Cloud Manager prompts you to subscribe to the annual contract that's available in the AWS Marketplace.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the annual contract in the AWS Marketplace.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☒ **Pay-Per-TiB - Annual Contract**

Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☐ **Pay-as-you-go**

Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace

Subscribe and then click **Set Up Your Account** to configure your account.

2 Cloud Manager

Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

Cancel

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

Select Charging Method

☒ **Professional**

By capacity



☐ **Essential**

By capacity



☐ **Freemium (Up to 500 GiB)**

By capacity



☐ **Per Node**

By node



[View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.](#)

Keystone Flex Subscription

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. [Learn more about Keystone Flex Subscriptions.](#)

Steps

1. If you don't have a subscription yet, [contact NetApp](#)
2. [Contact NetApp](#) to authorize your Cloud Manager user account with one or more Keystone Flex Subscriptions.
3. After NetApp authorizes your account, [link your subscriptions for use with Cloud Volumes ONTAP](#).
4. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - a. Select the Keystone Flex Subscription charging method when prompted to choose a charging method.

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

☐ Professional By capacity v

☐ Essential By capacity v

☐ Freemium (Up to 500 GiB) By capacity v

☐ Per Node By node v

[View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.](#)

Launching Cloud Volumes ONTAP in AWS

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

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](#).
- An understanding of the configuration that you want to use.

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

- DNS and Active Directory for CIFS configurations.

For details, see [Networking requirements for Cloud Volumes ONTAP in AWS](#).

Launching a single-node Cloud Volumes ONTAP system in AWS

If you want to launch Cloud Volumes ONTAP in AWS, you need to create a new working environment in Cloud Manager.

About this task

Immediately after you create the working environment, Cloud Manager launches a test instance in the specified VPC to verify connectivity. If successful, Cloud Manager immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If Cloud Manager cannot verify connectivity, creation of the working environment fails. The test instance is either a t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Amazon Web Services** and **Cloud Volumes ONTAP Single Node**.
3. If you're prompted, [create a Connector](#).
4. **Details and Credentials:** Optionally change the AWS credentials and subscription, enter a working environment name, add tags if needed, and then enter a password.

Some of the fields in this page are self-explanatory. 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 Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option. |

| Field | Description |
|------------------------|--|
| Add tags | <p>AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance.</p> <p>You can add up to four tags 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 tags when creating a working environment.</p> <p>For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.</p> |
| User name and password | <p>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name.</p> |
| Edit Credentials | <p>Choose the AWS credentials associated with the account where you want to deploy this system. You can also associate the AWS Marketplace subscription to use with this Cloud Volumes ONTAP system.</p> <p>Click Add Subscription to associate the selected credentials with a new AWS Marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate.</p> <p>Learn how to add additional AWS credentials to Cloud Manager.</p> |

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

► https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4


(video)



If multiple IAM users work in the same AWS account, then each user needs to subscribe. After the first user subscribes, the AWS Marketplace informs subsequent users that they're already subscribed, as shown in the image below. While a subscription is in place for the *AWS account*, each IAM user needs to associate themselves with that subscription. If you see the message shown below, click the **click here** link to go to Cloud Central and complete the process.

Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

**Having issues signing up for your product?**

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

[Subscribe](#)

You are already subscribed to this product

Pricing Details

Software Fees

5. **Services:** Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.

- [Learn more about Cloud Data Sense.](#)
- [Learn more about Cloud Backup.](#)
- [Learn more about Monitoring.](#)

6. **Location & Connectivity:** Enter the network information that you recorded in the [AWS worksheet](#).

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

| Field | Description |
|-----------------------------|--|
| VPC | If you have an AWS Outpost, you can deploy a single node Cloud Volumes ONTAP system in that Outpost by selecting the Outpost VPC. The experience is the same as any other VPC that resides in AWS. |
| Generated security group | <p>If you let Cloud Manager generate the security group for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none">• If you choose Selected VPC only, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.• If you choose All VPCs, the source for inbound traffic is the 0.0.0.0/0 IP range. |
| Use existing security group | <p>If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.</p> |

7. **Data Encryption:** Choose no data encryption or AWS-managed encryption.

For AWS-managed encryption, you can choose a different Customer Master Key (CMK) from your account or another AWS account.



You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

[Learn how to set up the AWS KMS for Cloud Volumes ONTAP.](#)

[Learn more about supported encryption technologies.](#)

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. **Cloud Volumes ONTAP Configuration** (annual AWS Marketplace contract only): Review the default configuration and click **Continue** or click **Change Configuration** to select your own configuration.

If you keep the default configuration, then you only need to specify a volume and then review and approve the configuration.

10. **Preconfigured Packages:** Select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Change Configuration** to select your own configuration.

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

11. **IAM Role:** It's best to keep the default option to let Cloud Manager create the role for you.

If you prefer to use your own policy, it must meet [policy requirements for Cloud Volumes ONTAP nodes](#).

12. **Licensing:** Change the Cloud Volumes ONTAP version as needed and select an instance type and the instance tenancy.



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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

13. **Underlying Storage Resources:** Choose a disk type, configure the underlying storage, and choose whether to keep data tiering enabled.

Note the following:

- The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).
- If you choose a gp3 or io1 disk, Cloud Manager uses the Elastic Volumes feature in AWS to automatically increase the underlying storage disk capacity as needed. You can choose the initial capacity based on your storage needs and revise it after Cloud Volumes ONTAP is deployed. [Learn more about support for Elastic Volumes in AWS.](#)
- If you choose a gp2 or st1 disk, you can select a disk size 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.
- 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.

[Learn how data tiering works.](#)

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

[Learn more about write speed.](#)

WORM can't be enabled if data tiering was enabled.

[Learn more about WORM storage.](#)

15. **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, 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. |

| Field | Description |
|---|--|
| 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 bus 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, use the IQN to connect to the LUN from your hosts.</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

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

| Field | Description |
|---|---|
| DNS Primary and Secondary IP Address | <p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p> |
| 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. |

| Field | Description |
|---------------------|---|
| Organizational Unit | The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter OU=Computers,OU=corp in this field. |
| 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. See the Cloud Manager automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server. |

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

For more information, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

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

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

Result

Cloud Manager launches the Cloud Volumes ONTAP instance. You can track the progress in the timeline.

If you experience any issues launching the Cloud Volumes ONTAP instance, 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 a Cloud Volumes ONTAP HA pair in AWS

If you want to launch a Cloud Volumes ONTAP HA pair in AWS, you need to create an HA working environment in Cloud Manager.

Limitation

At this time, HA pairs are not supported with AWS Outposts.

About this task

Immediately after you create the working environment, Cloud Manager launches a test instance in the specified VPC to verify connectivity. If successful, Cloud Manager immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If Cloud Manager cannot verify connectivity, creation of the working environment fails. The test instance is either a t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Amazon Web Services** and **Cloud Volumes ONTAP Single Node**.
3. **Details and Credentials:** Optionally change the AWS credentials and subscription, enter a working environment name, add tags if needed, and then enter a password.

Some of the fields in this page are self-explanatory. 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 Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option. |
| Add tags | <p>AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance.</p> <p>You can add up to four tags 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 tags when creating a working environment.</p> <p>For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.</p> |
| 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 System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name. |
| Edit Credentials | <p>Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system.</p> <p>Click Add Subscription to associate the selected credentials with a new AWS Marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate.</p> <p>If purchased a license directly from NetApp (BYOL), then an AWS subscription isn't required.</p> <p>Learn how to add additional AWS credentials to Cloud Manager.</p> |

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

► https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4

(video)



If multiple IAM users work in the same AWS account, then each user needs to subscribe. After the first user subscribes, the AWS Marketplace informs subsequent users that they're already subscribed, as shown in the image below. While a subscription is in place for the *AWS account*, each IAM user needs to associate themselves with that subscription. If you see the message shown below, click the **click here** link to go to Cloud Central and complete the process.

4. **Services:** Keep the services enabled or disable the individual services that you don't want to use with this Cloud Volumes ONTAP system.
 - [Learn more about Cloud Data Sense.](#)
 - [Learn more about Cloud Backup.](#)
 - [Learn more about Monitoring.](#)

5. **HA Deployment Models:** Choose an HA configuration.

For an overview of the deployment models, see [Cloud Volumes ONTAP HA for AWS](#).

6. **Location and Connectivity** (single AZ) or **Region & VPC** (multiple AZs): Enter the network information that you recorded in the AWS worksheet.

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

| Field | Description |
|-----------------------------|--|
| Generated security group | <p>If you let Cloud Manager generate the security group for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none">• If you choose Selected VPC only, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.• If you choose All VPCs, the source for inbound traffic is the 0.0.0.0/0 IP range. |
| Use existing security group | <p>If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.</p> |

7. **Connectivity and SSH Authentication:** Choose connection methods for the HA pair and the mediator.
8. **Floating IPs:** If you chose multiple AZs, specify the floating IP addresses.

The IP addresses must be outside of the CIDR block for all VPCs in the region. For additional details, see [AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs](#).

9. **Route Tables:** If you chose multiple AZs, select the route tables that should include routes to the floating IP addresses.

If you have more than one route table, it is very important to select the correct route tables. Otherwise, some clients might not have access to the Cloud Volumes ONTAP HA pair. For more information about route tables, refer to [AWS Documentation: Route Tables](#).

10. **Data Encryption:** Choose no data encryption or AWS-managed encryption.

For AWS-managed encryption, you can choose a different Customer Master Key (CMK) from your account or another AWS account.



You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

[Learn how to set up the AWS KMS for Cloud Volumes ONTAP.](#)

[Learn more about supported encryption technologies.](#)

11. **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.](#)

12. **Cloud Volumes ONTAP Configuration** (annual AWS Marketplace contract only): Review the default configuration and click **Continue** or click **Change Configuration** to select your own configuration.

If you keep the default configuration, then you only need to specify a volume and then review and approve the configuration.

13. **Preconfigured Packages** (hourly or BYOL only): Select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Change Configuration** to select your own configuration.

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

14. **IAM Role:** It's best to keep the default option to let Cloud Manager create the role for you.

If you prefer to use your own policy, it must meet [policy requirements for Cloud Volumes ONTAP nodes and the HA mediator](#).

15. **Licensing:** Change the Cloud Volumes ONTAP version as needed and select an instance type and the instance tenancy.



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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

16. **Underlying Storage Resources:** Choose a disk type, configure the underlying storage, and choose whether to keep data tiering enabled.

Note the following:

- The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).
- If you choose a gp3 or io1 disk, Cloud Manager uses the Elastic Volumes feature in AWS to automatically increase the underlying storage disk capacity as needed. You can choose the initial capacity based on your storage needs and revise it after Cloud Volumes ONTAP is deployed. [Learn](#)

[more about support for Elastic Volumes in AWS.](#)

- If you choose a gp2 or st1 disk, you can select a disk size 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.
- 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.

[Learn how data tiering works.](#)

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

[Learn more about write speed.](#)

WORM can't be enabled if data tiering was enabled.

[Learn more about WORM storage.](#)

18. **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, 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. |

| Field | Description |
|---|--|
| 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 bus 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, use the IQN to connect to the LUN from your hosts.</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

19. **CIFS Setup:** If you selected the CIFS protocol, set up a CIFS server.

| Field | Description |
|---|---|
| DNS Primary and Secondary IP Address | <p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p> |
| 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. |

| Field | Description |
|---------------------|---|
| Organizational Unit | The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter OU=Computers,OU=corp in this field. |
| 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. See the Cloud Manager automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server. |

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

For more information, see [Understanding volume usage profiles](#) and [Data tiering overview](#).

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

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

Result

Cloud Manager launches the Cloud Volumes ONTAP HA pair. You can track the progress in the timeline.

If you experience any issues launching the HA pair, 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.

Get started with Cloud Volumes ONTAP in the AWS C2S environment

Similar to a standard AWS region, you can use Cloud Manager in the [AWS Commercial Cloud Services \(C2S\)](#) environment to deploy Cloud Volumes ONTAP, which provides enterprise-class features for your cloud storage. AWS C2S is a closed region specific to the U.S. Intelligence Community; the instructions on this page only apply to AWS C2S

region users.

Supported features in C2S

The following features are available from Cloud Manager in the C2S environment:

- Cloud Volumes ONTAP
- Data replication
- A timeline for auditing

For Cloud Volumes ONTAP, you can create a single node system or an HA pair. Both licensing options are available: pay-as-you-go and bring your own license (BYOL).

Data tiering to S3 is also supported with Cloud Volumes ONTAP in C2S.

Limitations

- None of NetApp's cloud services are available from Cloud Manager.
- Because there's no internet access in the C2S environment, the following features aren't available either:
 - Integration with NetApp Cloud Central
 - Automated software upgrades from Cloud Manager
 - NetApp AutoSupport
 - AWS cost information for Cloud Volumes ONTAP resources
- Freemium licenses are not supported in the C2S environment.

Deployment overview

Getting started with Cloud Volumes ONTAP in C2S includes a few steps.

1. Preparing your AWS environment.

This includes setting up networking, subscribing to Cloud Volumes ONTAP, setting up permissions, and optionally setting up the AWS KMS.

2. Installing the Connector and setting up Cloud Manager.

Before you can start using Cloud Manager to deploy Cloud Volumes ONTAP, you'll need to create a *Connector*. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment (this includes Cloud Volumes ONTAP).

You'll log in to Cloud Manager from the software that gets installed on the Connector instance.

3. Launching Cloud Volumes ONTAP from Cloud Manager.

Each of these steps are described below.

Prepare your AWS environment

Your AWS environment must meet a few requirements.

Set up your networking

Set up your AWS networking so Cloud Volumes ONTAP can operate properly.

Steps

1. Choose the VPC and subnets in which you want to launch the Connector instance and Cloud Volumes ONTAP instances.
2. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
3. Set up a VPC endpoint to the S3 service.

A VPC endpoint is required if you want to tier cold data from Cloud Volumes ONTAP to low-cost object storage.

Subscribe to Cloud Volumes ONTAP

A Marketplace subscription is required to deploy Cloud Volumes ONTAP from Cloud Manager.

Steps

1. Go to the AWS Intelligence Community Marketplace and search for Cloud Volumes ONTAP.
2. Select the offering that you plan to deploy.
3. Review the terms and click **Accept**.
4. Repeat these steps for the other offerings, if you plan to deploy them.

You must use Cloud Manager to launch Cloud Volumes ONTAP instances. You must not launch Cloud Volumes ONTAP instances from the EC2 console.

Set up permissions

Set up IAM policies and roles that provide Cloud Manager and Cloud Volumes ONTAP with the permissions that they need to perform actions in the AWS Commercial Cloud Services environment.

You need an IAM policy and IAM role for each of the following:

- The Connector instance
- Cloud Volumes ONTAP instances
- The Cloud Volumes ONTAP HA mediator instance (if you want to deploy HA pairs)

Steps

1. Go to the AWS IAM console and click **Policies**.
2. Create a policy for the Connector instance.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
```

```
"ec2:DescribeInstanceStatus",
"ec2:RunInstances",
"ec2:ModifyInstanceAttribute",
"ec2:DescribeRouteTables",
"ec2:DescribeImages",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:DescribeVolumes",
"ec2:ModifyVolumeAttribute",
"ec2>DeleteVolume",
"ec2:CreateSecurityGroup",
"ec2>DeleteSecurityGroup",
"ec2:DescribeSecurityGroups",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2>DeleteNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeDhcpOptions",
"ec2:CreateSnapshot",
"ec2>DeleteSnapshot",
"ec2:DescribeSnapshots",
"ec2:GetConsoleOutput",
"ec2:DescribeKeyPairs",
"ec2:DescribeRegions",
"ec2>DeleteTags",
"ec2:DescribeTags",
"cloudformation:CreateStack",
"cloudformation>DeleteStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"iam:PassRole",
"iam:CreateRole",
"iam>DeleteRole",
"iam:PutRolePolicy",
"iam:ListInstanceProfiles",
"iam:CreateInstanceProfile",
"iam>DeleteRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
```

```

        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [

```

```

        "arn:aws-iso:ec2:*:*:instance/*"
    ],
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso:ec2:*:*:volume/*"
        ]
    }
]
}

```

3. Create a policy for Cloud Volumes ONTAP.

```

{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3>DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }
    ]
}

```

4. If you plan to deploy a Cloud Volumes ONTAP HA pair, create a policy for the HA mediator.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }]
}

```

5. Create IAM roles with the role type Amazon EC2 and attach the policies that you created in the previous steps.

Similar to the policies, you should have one IAM role for the Connector, one for the Cloud Volumes ONTAP nodes, and one for the HA mediator (if you want to deploy HA pairs).

You must select the Connector IAM role when you launch the Connector instance.

You can select the IAM roles for Cloud Volumes ONTAP and the HA mediator when you create a Cloud Volumes ONTAP working environment from Cloud Manager.

Set up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, ensure that requirements are met for the AWS Key Management Service.

Steps

1. Ensure that an active Customer Master Key (CMK) exists in your account or in another AWS account.

The CMK can be an AWS-managed CMK or a customer-managed CMK.

2. If the CMK is in an AWS account separate from the account where you plan to deploy Cloud Volumes ONTAP, then you need to obtain the ARN of that key.

You'll need to provide the ARN to Cloud Manager when you create the Cloud Volumes ONTAP system.

3. Add the IAM role for the Cloud Manager instance to the list of key users for a CMK.

This gives Cloud Manager permissions to use the CMK with Cloud Volumes ONTAP.

Install and set up Cloud Manager

Before you can launch Cloud Volumes ONTAP systems in AWS, you must first launch the Connector instance from the AWS Marketplace and then log in and set up Cloud Manager.

Steps

1. Obtain a root certificate signed by a certificate authority (CA) in the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. Consult your organization's policies and procedures for obtaining the certificate.

You'll need to upload the certificate during the setup process. Cloud Manager uses the trusted certificate when sending requests to AWS over HTTPS.

2. Launch the Connector instance:
 - a. Go to the AWS Intelligence Community Marketplace page for Cloud Manager.
 - b. On the Custom Launch tab, choose the option to launch the instance from the EC2 console.
 - c. Follow the prompts to configure the instance.

Note the following as you configure the instance:

- We recommend t3.xlarge.
- You must choose the IAM role that you created when preparing your AWS environment.
- You should keep the default storage options.
- The required connection methods for the Connector are as follows: SSH, HTTP, and HTTPS.

3. Set up Cloud Manager from a host that has a connection to the Connector instance:
 - a. Open a web browser and enter the following URL: <http://ipaddress:80>
 - b. Specify a proxy server for connectivity to AWS services.
 - c. Upload the certificate that you obtained in step 1.
 - d. Complete the steps in the Setup wizard to set up Cloud Manager.
 - **System Details:** Enter a name for this instance of Cloud Manager and provide your company name.
 - **Create User:** Create the Admin user that you'll use to administer Cloud Manager.
 - **Review:** Review the details and approve the end user license agreement.
 - e. To complete installation of the CA-signed certificate, restart the Connector instance from the EC2 console.
4. After the Connector restarts, log in using the administrator user account that you created in the Setup wizard.

Launch Cloud Volumes ONTAP

You can launch Cloud Volumes ONTAP instances in the AWS Commercial Cloud Services environment by creating new working environments in Cloud Manager.

What you'll need

- If you purchased a license, you must have the license file that you received from NetApp. The license file is a .NLF file in JSON format.
- A key pair is required to enable key-based SSH authentication to the HA mediator.

Steps

1. On the Working Environments page, click **Add Working Environment**.
2. Under Create, select Cloud Volumes ONTAP or Cloud Volumes ONTAP HA.
3. Complete the steps in the wizard to launch the Cloud Volumes ONTAP system.

Note the following as you complete the wizard:

- If you want to deploy Cloud Volumes ONTAP HA in multiple Availability Zones, deploy the configuration as follows because only two AZs were available in the AWS Commercial Cloud Services environment at the time of publication:
 - Node 1: Availability Zone A
 - Node 2: Availability Zone B
 - Mediator: Availability Zone A or B
- You should leave the default option to use a generated security group.

The predefined security group includes the rules that Cloud Volumes ONTAP needs to operate successfully. If you have a requirement to use your own, you can refer to the security group section below.

- You must choose the IAM role that you created when preparing your AWS environment.
- The underlying AWS disk type is for the initial Cloud Volumes ONTAP volume.

You can choose a different disk type for subsequent volumes.

- The performance of AWS disks is tied to disk size.

You should choose the disk size that gives you the sustained performance that you need. Refer to AWS documentation for more details about EBS performance.

- The disk size is the default size for all disks on the system.



If you need a different size later, you can use the Advanced allocation option to create an aggregate that uses disks of a specific size.

- Storage efficiency features can improve storage utilization and reduce the total amount of storage that you need.

Result

Cloud Manager launches the Cloud Volumes ONTAP instance. You can track the progress in the timeline.

Security group rules

Cloud Manager creates security groups that include the inbound and outbound rules that Cloud Manager and Cloud Volumes ONTAP need to operate successfully in the cloud. You might want to refer to the ports for testing purposes or if you prefer to use your own security groups.

Security group for the Connector

The security group 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 security group for the Connector includes the following outbound rules.

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

Security group for Cloud Volumes ONTAP

The security group for Cloud Volumes ONTAP nodes requires both inbound and outbound rules.

Inbound rules

When you create a working environment and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VPC only:** the source 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 Connector resides. This is the recommended option.
- **All VPCs:** the source for inbound traffic is the 0.0.0.0/0 IP range.

| 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 |
| 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 |

| Protocol | Port | Purpose |
|----------|---------|--|
| 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 |
| 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 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 |

External security group for the HA mediator

The predefined external security group for the Cloud Volumes ONTAP HA mediator includes the following inbound and outbound rules.

Inbound rules

The source for inbound rules is traffic from the VPC where the Connector resides.

| Protocol | Port | Purpose |
|----------|------|---------------------------------------|
| SSH | 22 | SSH connections to the HA mediator |
| TCP | 3000 | RESTful API access from the Connector |

Outbound rules

The predefined security group for the HA mediator includes the following outbound rules.

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

Internal security group for the HA mediator

The predefined internal security group for the Cloud Volumes ONTAP HA mediator includes the following rules. Cloud Manager always creates this security group. You don't have the option to use your own.

Inbound rules

The predefined security group includes the following inbound rules.

| Protocol | Port | Purpose |
|-------------|------|--|
| All traffic | All | Communication between the HA mediator and HA nodes |

Outbound rules

The predefined security group includes the following outbound rules.

| Protocol | Port | Purpose |
|-------------|------|--|
| All traffic | All | Communication between the HA mediator and HA nodes |

Get started in Microsoft Azure

Quick start for Cloud Volumes ONTAP in Azure

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

1

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 Azure.](#)

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.

2

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.](#)

3

Set up your networking

- a. Ensure that your VNet and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
- b. Enable outbound internet access from the target VNet 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.](#)



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

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

Plan your Cloud Volumes ONTAP configuration in Azure

When you deploy Cloud Volumes ONTAP in Azure, 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 Microsoft Azure regions. [View the full list of supported regions.](#)

Choose a supported VM type

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

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

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 Azure

Size your system in Azure

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 VM type, disk type, and disk size:

Virtual machine type

Look at the supported virtual machine types in the [Cloud Volumes ONTAP Release Notes](#) and then review details about each supported VM type. Be aware that each VM type supports a specific number of data disks.

- [Azure documentation: General purpose virtual machine sizes](#)
- [Azure documentation: Memory optimized virtual machine sizes](#)

Azure disk type

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses as a disk.

HA systems use Premium page blobs. Meanwhile, single node systems can use two types of Azure Managed Disks:

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.
- *Standard SSD Managed Disks* provide consistent performance for workloads that require low IOPS.
- *Standard HDD Managed Disks* are a good choice if you don't need high IOPS and want to reduce your costs.

For additional details about the use cases for these disks, see [Microsoft Azure Documentation: What disk types are available in Azure?](#)

Azure disk size

When you launch Cloud Volumes ONTAP instances, you must choose the default disk size for aggregates. Cloud Manager uses this disk size for the initial aggregate, and for any additional aggregates that it creates when you use the simple provisioning option. You can create aggregates that use a disk size different from the default by [using the advanced allocation option](#).



All disks in an aggregate must be the same size.

When choosing a disk size, you should take several factors into consideration. The disk size impacts how much you pay for storage, the size of volumes that you can create in an aggregate, the total capacity available to Cloud Volumes ONTAP, and storage performance.

The performance of Azure Premium Storage is tied to the disk size. Larger disks provide higher IOPS and throughput. For example, choosing 1 TiB disks can provide better performance than 500 GiB disks, at a higher cost.

There are no performance differences between disk sizes for Standard Storage. You should choose disk

size based on the capacity that you need.

Refer to Azure for IOPS and throughput by disk size:

- [Microsoft Azure: Managed Disks pricing](#)
- [Microsoft Azure: Page Blobs pricing](#)

View default system disks

In addition to the storage for user data, Cloud Manager 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 Azure.](#)



The Connector also requires a system disk. [View details about the Connector's default configuration.](#)

Collect networking information

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

| Azure information | Your value |
|--|------------|
| Region | |
| Virtual network (VNet) | |
| Subnet | |
| Network security group (if using your own) | |

Choose a write speed

Cloud Manager enables you to choose a write speed setting for Cloud Volumes ONTAP. 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 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 Azure

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

Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

Outbound internet access

Cloud Volumes ONTAP nodes require outbound internet access for NetApp AutoSupport, which proactively monitors the health of your system and sends messages to NetApp technical support.

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>

If an outbound internet connection isn't available to send AutoSupport messages, Cloud Manager automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server. The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you defined strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

After you've verified that outbound internet access is available, you can test AutoSupport to ensure that it can send messages. For instructions, refer to [ONTAP docs: Set up AutoSupport](#).

If Cloud Manager notifies you that AutoSupport messages can't be sent, [troubleshoot your AutoSupport configuration](#).

IP addresses

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

- Single node: 5 IP addresses
- HA pair: 16 IP addresses

Note that Cloud Manager creates an SVM management LIF on HA pairs, but not on single node systems in Azure.



A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

Secure connections to Azure services

By default, Cloud Manager enables an Azure Private Link for connections between Cloud Volumes ONTAP and Azure storage accounts.

In most cases, there's nothing that you need to do—Cloud Manager manages the Azure Private Link for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You should also be aware of a requirement for the Connector location in Azure.

You can also disable the Private Link connection, if required by your business needs. If you disable the link, Cloud Manager configures Cloud Volumes ONTAP to use a service endpoint instead.

[Learn more about using Azure Private Links or service endpoints with Cloud Volumes ONTAP.](#)

Connections to other ONTAP systems

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

For instructions, refer to [Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal](#).

Port for the HA interconnect

A Cloud Volumes ONTAP HA pair includes an HA interconnect, which allows each node to continually check whether its partner is functioning and to mirror log data for the other's nonvolatile memory. The HA interconnect uses TCP port 10006 for communication.

By default, communication between the HA interconnect LIFs is open and there are no security group rules for this port. But if you create a firewall between the HA interconnect LIFs, then you need to ensure that TCP traffic is open for port 10006 so that the HA pair can operate properly.

Only one HA pair in an Azure resource group

You must use a *dedicated* resource group for each Cloud Volumes ONTAP HA pair that you deploy in Azure. Only one HA pair is supported in a resource group.

Cloud Manager experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group.

Security groups

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

Security group rules

Cloud Manager creates Azure security groups 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 security groups.

The security group for Cloud Volumes ONTAP requires both inbound and outbound rules.

Inbound rules for single node systems

When you create a working environment and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VNet only:** the source for inbound traffic is the subnet range of the VNet for the Cloud Volumes ONTAP system and the subnet range of the VNet where the Connector resides. This is the recommended option.
- **All VNets:** the source for inbound traffic is the 0.0.0.0/0 IP range.

| Priority and name | Port and protocol | Source and destination | Description |
|-----------------------------|-------------------|------------------------|---|
| 1000 inbound_ssh | 22 TCP | Any to Any | SSH access to the IP address of the cluster management LIF or a node management LIF |
| 1001 inbound_http | 80 TCP | Any to Any | HTTP access to the System Manager web console using the IP address of the cluster management LIF |
| 1002 inbound_111_tcp | 111 TCP | Any to Any | Remote procedure call for NFS |
| 1003 inbound_111_udp | 111 UDP | Any to Any | Remote procedure call for NFS |
| 1004 inbound_139 | 139 TCP | Any to Any | NetBIOS service session for CIFS |
| 1005 inbound_161-162_tcp | 161-162 TCP | Any to Any | Simple network management protocol |
| 1006 inbound_161-162_udp | 161-162 UDP | Any to Any | Simple network management protocol |
| 1007 inbound_443 | 443 TCP | Any to Any | Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF |
| 1008 inbound_445 | 445 TCP | Any to Any | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| 1009 inbound_635_tcp | 635 TCP | Any to Any | NFS mount |
| 1010 inbound_635_udp | 635 UDP | Any to Any | NFS mount |
| 1011 inbound_749 | 749 TCP | Any to Any | Kerberos |
| 1012 inbound_2049_tcp | 2049 TCP | Any to Any | NFS server daemon |
| 1013 inbound_2049_udp | 2049 UDP | Any to Any | NFS server daemon |

| Priority and name | Port and protocol | Source and destination | Description |
|--|--------------------------|----------------------------------|--|
| 1014 inbound_3260 | 3260 TCP | Any to Any | iSCSI access through the iSCSI data LIF |
| 1015 inbound_4045-4046_tcp | 4045-4046 TCP | Any to Any | NFS lock daemon and network status monitor |
| 1016 inbound_4045-4046_udp | 4045-4046 UDP | Any to Any | NFS lock daemon and network status monitor |
| 1017 inbound_10000 | 10000 TCP | Any to Any | Backup using NDMP |
| 1018 inbound_11104-11105 | 11104-11105 TCP | Any to Any | SnapMirror data transfer |
| 3000 inbound_deny_all_tcp | Any port TCP | Any to Any | Block all other TCP inbound traffic |
| 3001 inbound_deny_all_udp | Any port UDP | Any to Any | Block all other UDP inbound traffic |
| 65000 AllowVnetInBound | Any port Any protocol | VirtualNetwork to VirtualNetwork | Inbound traffic from within the VNet |
| 65001 AllowAzureLoadBalancerInBound | Any port Any protocol | AzureLoadBalancer to Any | Data traffic from the Azure Standard Load Balancer |
| 65500 DenyAllInBound | Any port Any protocol | Any to Any | Block all other inbound traffic |

Inbound rules for HA systems

When you create a working environment and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VNet only:** the source for inbound traffic is the subnet range of the VNet for the Cloud Volumes ONTAP system and the subnet range of the VNet where the Connector resides. This is the recommended option.
- **All VNets:** the source for inbound traffic is the 0.0.0.0/0 IP range.



HA systems have less inbound rules than single node systems because inbound data traffic goes through the Azure Standard Load Balancer. Because of this, traffic from the Load Balancer should be open, as shown in the "AllowAzureLoadBalancerInBound" rule.

| Priority and name | Port and protocol | Source and destination | Description |
|--|--------------------------|----------------------------------|---|
| 100 inbound_443 | 443 Any protocol | Any to Any | Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF |
| 101 inbound_111_tcp | 111 Any protocol | Any to Any | Remote procedure call for NFS |
| 102 inbound_2049_tcp | 2049 Any protocol | Any to Any | NFS server daemon |
| 111 inbound_ssh | 22 Any protocol | Any to Any | SSH access to the IP address of the cluster management LIF or a node management LIF |
| 121 inbound_53 | 53 Any protocol | Any to Any | DNS and CIFS |
| 65000 AllowVnetInBound | Any port Any protocol | VirtualNetwork to VirtualNetwork | Inbound traffic from within the VNet |
| 65001 AllowAzureLoadBalancerInBound | Any port Any protocol | AzureLoadBalancer to Any | Data traffic from the Azure Standard Load Balancer |
| 65500 DenyAllInBound | Any port Any protocol | Any to Any | Block all other inbound traffic |

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.

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

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

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](#).

Connections to target networks

A Connector requires a network connection to the VPCs and VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the VPC or VNet in which you launch Cloud Volumes ONTAP.

Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment.

| Endpoints | Purpose |
|--|---|
| https://support.netapp.com | To obtain licensing information and to send AutoSupport messages to NetApp support. |
| https://*.cloudmanager.cloud.netapp.com | To provide SaaS features and services within Cloud Manager. |
| https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net | To upgrade the Connector and its Docker components. |

Security group rules

The security group for the Connector requires both inbound and outbound rules.

Inbound rules

| Port | Protocol | Purpose |
|------|----------|---|
| 22 | SSH | Provides SSH access to the Connector host |
| 80 | HTTP | Provides HTTP access from client web browsers to the local user interface |
| 443 | HTTPS | Provides HTTPS access from client web browsers to the local user interface |
| TCP | 3128 | Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deploying the Connector. |

Outbound rules

The predefined security group 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 security group for the Connector includes the following outbound rules.

| Port | Protocol | Purpose |
|------|----------|----------------------|
| All | All TCP | All outbound traffic |
| All | All UDP | 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 | Port | Protocol | Destination | Purpose |
|---------------------------|------|----------|--|--|
| API calls and AutoSupport | 443 | HTTPS | Outbound internet and ONTAP cluster management LIF | API calls to Azure and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |
| DNS | 53 | UDP | DNS | Used for DNS resolve by Cloud Manager |

Set up Cloud Volumes ONTAP to use a customer-managed key in Azure

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using [Azure Storage Service Encryption](#) with a Microsoft-managed key. But you can use your own encryption key instead by following the steps on this page.

Data encryption overview

Cloud Volumes ONTAP data is automatically encrypted in Azure using [Azure Storage Service Encryption](#). The default implementation uses a Microsoft-managed key. No setup is required.

If you want to use a customer-managed key with Cloud Volumes ONTAP, then you need to complete the following steps:

1. From Azure, create a key vault and then generate a key in that vault
2. From Cloud Manager, use the API to create a Cloud Volumes ONTAP working environment that uses the key

Key rotation

If you create a new version of your key, Cloud Volumes ONTAP automatically uses the latest key version.

How data is encrypted

After you create a Cloud Volumes ONTAP working environment that is configured to use a customer-managed key, Cloud Volumes ONTAP data is encrypted as follows.

HA pairs

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.

- Any new storage accounts (for example, when you add disks or aggregates) also use the same key.

Single node

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.
- For root, boot, and data disks, Cloud Manager uses a [disk encryption set](#), which enables management of encryption keys with managed disks.
- Any new data disks also use the same disk encryption set.
- NVRAM and the core disk are encrypted using a Microsoft-managed key, instead of the customer-managed key.

Create a key vault and generate a key

The key vault must reside in the same Azure subscription and region in which you plan to create the Cloud Volumes ONTAP system.

Steps

1. [Create a key vault in your Azure subscription.](#)

Note the following requirements for the key vault:

- The key vault must reside in the same region as the Cloud Volumes ONTAP system.
- The following options should be enabled:
 - **Soft-delete** (this option is enabled by default, but must *not* be disabled)
 - **Purge protection**
 - **Azure Disk Encryption for volume encryption** (for single node Cloud Volumes ONTAP systems only)

2. [Generate a key in the key vault.](#)

Note the following requirements for the key:

- The key type must be **RSA**.
- The recommended RSA key size is **2048**, but other sizes are supported.

Create a working environment that uses the encryption key

After you create the key vault and generate an encryption key, you can create a new Cloud Volumes ONTAP system that is configured to use the key. These steps are supported by using the Cloud Manager API.

Required permissions

If you want to use a customer-managed key with a single node Cloud Volumes ONTAP system, ensure that the Cloud Manager Connector has the following permissions:

```
"Microsoft.Compute/diskEncryptionSets/read"
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write"
```

[View the latest list of permissions](#)



The first three permissions aren't required for HA pairs.

Steps

1. Obtain the list of key vaults in your Azure subscription by using the following Cloud Manager API call.

For an HA pair: GET /azure/ha/metadata/vaults

For single node: GET /azure/vsa/metadata/vaults

Make note of the **name** and **resourceGroup**. You'll need to specify those values in the next step.

[Learn more about this API call.](#)

2. Obtain the list of keys within the vault by using the following Cloud Manager API call.

For an HA pair: GET /azure/ha/metadata/keys-vault

For single node: GET /azure/vsa/metadata/keys-vault

Make note of the **keyName**. You'll need to specify that value (along with the vault name) in the next step.

[Learn more about this API call.](#)

3. Create a Cloud Volumes ONTAP system by using the following Cloud Manager API call.

- a. For an HA pair:

POST /azure/ha/working-environments

The request body must include the following fields:

```
"azureEncryptionParameters": {
  "key": "keyName",
  "vaultName": "vaultName"
}
```

[Learn more about this API call.](#)

- b. For a single node system:

POST /azure/vsa/working-environments

The request body must include the following fields:

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```

[Learn more about this API call.](#)

Result

You have a new Cloud Volumes ONTAP system that is configured to use your customer-managed key for data encryption.

Set up licensing for Cloud Volumes ONTAP in Azure

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 working environment.

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. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Azure 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](#).

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

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

Select Charging Method

| | | | |
|----------------------------------|--------------------------|-------------|---|
| <input type="radio"/> | Professional | By capacity | ▼ |
| <input type="radio"/> | Essential | By capacity | ▼ |
| <input checked="" type="radio"/> | Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> | Per Node | By node | ▼ |

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)

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 package or the Professional package.

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

- A license (BYOL) purchased from NetApp
- An hourly, pay-as-you-go (PAYGO) subscription from the Azure 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.

Steps

1. [Contact NetApp Sales to obtain a license](#)
2. [Add your NetApp Support Site account to Cloud Manager](#)

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

Your license must be available from the Digital Wallet before you can use it with Cloud Volumes ONTAP. If needed, you can [manually add the license to the Digital Wallet](#).

3. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Azure 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.

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+

 Add Subscription

Apply

Cancel

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

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)

PAYGO subscription

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

When you create a Cloud Volumes ONTAP working environment, Cloud Manager prompts you to subscribe to the agreement that's available in the Azure Marketplace. That subscription is then associated with the working

environment for charging. You can use that same subscription for additional working environments.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Azure Marketplace.

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". It has a section "Associate Subscription to Credentials" with a help icon. Below this are two dropdown menus: "Credentials" set to "Managed Service Identity" and "Azure Subscription" set to "OCCM Dev (Default)". A message box states: "Marketplace Subscription: A marketplace subscription isn't associated with the selected Azure subscription." Below the message is a "+ Add Subscription" link. At the bottom are "Apply" and "Cancel" buttons.

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

The screenshot shows a page titled "Select Charging Method". It lists four options with radio buttons: "Professional" (selected), "Essential", "Freemium (Up to 500 GiB)", and "Per Node". To the right of each option is a button labeled "By capacity" (for the first three) or "By node" (for the last one), followed by a dropdown arrow.

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)



You can manage the Azure Marketplace subscriptions associated with your Azure accounts from the Settings > Credentials page. [Learn how to manage your Azure accounts 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 Azure Marketplace.

After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Azure Marketplace during working environment creation.

2. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription > Continue**.
 - b. In the Azure portal, select the annual plan that was shared with your Azure account and then click **Subscribe**.
 - c. After you return to Cloud Manager, select a capacity-based package when you reach the charging methods page.

| Select Charging Method | |
|--|-------------|
| <input checked="" type="radio"/> Professional | By capacity |
| <input type="radio"/> Essential | By capacity |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity |
| <input type="radio"/> Per Node | By node |

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)

Keystone Flex Subscription

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. [Learn more about Keystone Flex Subscriptions.](#)

Steps

1. If you don't have a subscription yet, [contact NetApp](#)
2. [Contact NetApp](#) to authorize your Cloud Manager user account with one or more Keystone Flex

Subscriptions.

3. After NetApp authorizes your account, [link your subscriptions for use with Cloud Volumes ONTAP](#).
4. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - a. Select the Keystone Flex Subscription charging method when prompted to choose a charging method.

The screenshot shows a 'Select Charging Method' dialog box. The 'Keystone' option is selected, indicated by a blue checkmark. Below this, the text 'Storage management' and 'Charged against your NetApp credit' is displayed. A 'Keystone Subscription' dropdown menu is shown with 'A-AMRITA1' selected. To the right of the 'Keystone' option is a blue button labeled 'By capacity' and an upward-pointing chevron. Below the 'Keystone' option are four other options, each with a radio button: 'Professional', 'Essential', 'Freemium (Up to 500 GiB)', and 'Per Node'. To the right of each of these options is a blue button labeled 'By capacity' (for the first three) or a purple button labeled 'By node' (for 'Per Node'), and a downward-pointing chevron.

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)

Enable high availability mode in Azure

Microsoft Azure's high availability mode should be enabled to reduce unplanned failover times and to enable NFSv4 support for Cloud Volumes ONTAP.

Starting with the Cloud Volumes ONTAP 9.10.1 release, we reduced the unplanned failover time for Cloud Volumes ONTAP HA pairs running in Microsoft Azure and added support for NFSv4. To make these enhancements available to Cloud Volumes ONTAP, you need to enable the high availability feature on your Azure subscription.

Cloud Manager will prompt you with these details in an Action Required message when the feature needs to be enabled on an Azure subscription.

Note the following:

- There are no problems with the high availability of your Cloud Volumes ONTAP HA pair. This Azure feature works in concert with ONTAP to reduce the client observed application outage time for NFS protocols that result from unplanned failover events.

- Enabling this feature is non-disruptive to Cloud Volumes ONTAP HA pairs.
- Enabling this feature on your Azure subscription won't cause issues to other VMs.

An Azure user who has "Owner" privileges can enable the feature from the Azure CLI.

Steps

1. [Access the Azure Cloud Shell from the Azure Portal](#)
2. Register the high availability mode feature:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Optionally verify that the feature is now registered:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

The Azure CLI should return a result similar to the following:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Launching Cloud Volumes ONTAP in Azure

You can launch a single node system or an HA pair in Azure by creating a Cloud Volumes ONTAP working environment in Cloud Manager.

What you'll need

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](#).

- An understanding of the configuration that you want to use.

You should have chose a configuration and obtained Azure networking information from your administrator. For details, see [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](#).

About this task

When Cloud Manager creates a Cloud Volumes ONTAP system in Azure, it creates several Azure objects, such as a resource group, network interfaces, and storage accounts. You can review a summary of the resources at the end of the wizard.



Potential for Data Loss

The best practice is to use a new, dedicated resource group for each Cloud Volumes ONTAP system.

Deploying Cloud Volumes ONTAP in an existing, shared resource group is not recommended due to the risk of data loss. While Cloud Manager can remove Cloud Volumes ONTAP resources from a shared resource group in case of deployment failure or deletion, an Azure user might accidentally delete Cloud Volumes ONTAP resources from a shared resource group.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location:** Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node** or **Cloud Volumes ONTAP High Availability**.
3. If you're prompted, [create a Connector](#).
4. **Details and Credentials:** Optionally change the Azure credentials and subscription, specify a cluster name, add tags if needed, 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 Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option. |
| Resource Group Tags | <p>Tags are metadata for your Azure resources. When you enter tags in this field, Cloud Manager adds them to the resource group associated with the Cloud Volumes ONTAP system.</p> <p>You can add up to four tags 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 tags when creating a working environment.</p> <p>For information about tags, refer to Microsoft Azure Documentation: Using tags to organize your Azure resources.</p> |

| 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 System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name. |
| Edit Credentials | You can choose different Azure credentials and a different Azure subscription to use with this Cloud Volumes ONTAP system. You need to associate an Azure Marketplace subscription with the selected Azure subscription in order to deploy a pay-as-you-go Cloud Volumes ONTAP system. Learn how to add credentials. |

The following video shows how to associate a Marketplace subscription to an Azure subscription:

► <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes->

5. **Services:** Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.


- [Learn more about Cloud Data Sense.](#)
- [Learn more about Cloud Backup.](#)
- [Learn more about the Monitoring service.](#)

6. **Location:** Select a region, availability zone, VNet, and subnet, and then select the checkbox to confirm network connectivity between the Connector and the target location.

For single node systems, you can choose the Availability Zone in which you'd like to deploy Cloud Volumes ONTAP. If you don't select an AZ, Cloud Manager will select one for you.

7. **Connectivity:** Choose a new or existing resource group and then choose whether to use the predefined security group or to use your own.

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

| Field | Description |
|--------------------------|--|
| Availability Zone | For single node systems, you can choose the Availability Zone in which you'd like to deploy Cloud Volumes ONTAP. If you don't select an AZ, Cloud Manager will select one for you. |
| Resource Group | <p>Create a new resource group for Cloud Volumes ONTAP or use an existing resource group. The best practice is to use a new, dedicated resource group for Cloud Volumes ONTAP. While it is possible to deploy Cloud Volumes ONTAP in an existing, shared resource group, it's not recommended due to the risk of data loss. See the warning above for more details.</p> <p>You must use a dedicated resource group for each Cloud Volumes ONTAP HA pair that you deploy in Azure. Only one HA pair is supported in a resource group. Cloud Manager experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group.</p> <div> If the Azure account that you're using has the required permissions, Cloud Manager removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.</div> |
| Generated security group | <p>If you let Cloud Manager generate the security group for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none">• If you choose Selected VNet only, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Connector resides. This is the recommended option.• If you choose All VNets, the source for inbound traffic is the 0.0.0.0/0 IP range. |
| Use existing | If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. View the default security group. |

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 virtual machine type.



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 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

11. **Subscribe from the Azure Marketplace:** Follow the steps if Cloud Manager could not enable programmatic deployments of Cloud Volumes ONTAP.
12. **Underlying Storage Resources:** Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering to Blob storage should be enabled.

Note the following:

- 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 Azure](#).

- 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.

[Learn more about data tiering.](#)

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

[Learn more about write speed.](#)

WORM can't be enabled if data tiering was enabled.

[Learn more about WORM storage.](#)

14. **Secure Communication to Storage & WORM** (HA only): Choose whether to enable an HTTPS connection to Azure storage accounts, and activate write once, read many (WORM) storage, if desired.

The HTTPS connection is from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

[Learn more about WORM storage.](#)

15. **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, 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 bus 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, use the IQN to connect to the LUN from your hosts.</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

16. **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. 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. To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter OU=AADDCC Computers or OU=AADDCC Users in this field. Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain |
| 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. See the Cloud Manager automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server. |

17. **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](#).

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

- a. Review details about the configuration.
- b. Click **More information** to review details about support and the Azure 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.

Get started in Google Cloud

Quick start for Cloud Volumes ONTAP in Google Cloud

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

1

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.

2

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](#).

3

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.](#)

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 [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.](#)

5

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

6

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

- [Creating a Connector from Cloud Manager](#)
- [Installing the Connector software on a Linux host](#)

- [What Cloud Manager does with GCP permissions](#)

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 GCP](#)

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 GCP](#)

Size 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](#)

View default system disks

In addition to the storage for user data, Cloud Manager 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: Resource quotas](#)

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 Connector also requires a system disk. [View details about the Connector's default configuration.](#)

Collect networking information

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 | |

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

Choose 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.](#)

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 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 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.

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](#).

[Review the required shared VPC permissions covered in Connector deployment](#)

Packet mirroring in VPCs

[Packet mirroring](#) must be disabled in the Google Cloud VPC in which you deploy Cloud Volumes ONTAP. Cloud Volumes ONTAP can't operate properly if packet mirroring is enabled.

Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access for NetApp AutoSupport, which proactively monitors the health of your system and sends messages to NetApp technical support.

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>

If an outbound internet connection isn't available to send AutoSupport messages, Cloud Manager automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server. The only requirement is to ensure that the Connector's firewall allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you defined strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP firewall allows *outbound* connections over port 3128.

After you've verified that outbound internet access is available, you can test AutoSupport to ensure that it can send messages. For instructions, refer to [ONTAP docs: Set up AutoSupport](#).



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

If Cloud Manager notifies you that AutoSupport messages can't be sent, [troubleshoot your AutoSupport configuration](#).

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:** 14 or 15 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 VPC-0 only.

If you plan to deploy Cloud Volumes ONTAP in a VPC separate from the Connector, then you'll need to set up VPC Network Peering. [Learn more about VPC Network Peering](#)

Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment.

| Endpoints | Purpose |
|--|---|
| https://support.netapp.com | To obtain licensing information and to send AutoSupport messages to NetApp support. |
| https://*.cloudmanager.cloud.netapp.com | To provide SaaS features and services within Cloud Manager. |
| https://cloudmanagerinfraprod.azurecr.io | To upgrade the Connector and its Docker components. |
| https://*.blob.core.windows.net | |

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

When you create a working environment, 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 Connector 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 [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 | Connectivity with the Connector and 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 |
| 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 |

| Protocol | Port | Purpose |
|----------|-------------|--|
| 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 |
|-------------|-------------|-------------|--|----------------------------|--|
| AutoSupport | HTTPS | 443 | Node management LIF | support.netapp.com | AutoSupport (HTTPS is the default) |
| | HTTP | 80 | Node management LIF | support.netapp.com | AutoSupport (only if the transport protocol is changed from HTTPS to HTTP) |
| | TCP | 3128 | Node management LIF | Connector | Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available |
| Cluster | All traffic | All traffic | All LIFs on one node | All LIFs on the other node | Intercluster communications (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 | 1860-18699 | 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 |

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 rules 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 |
| TCP | 3128 | Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deploying the Connector. |

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 |
|---------------------------|----------|------|--|--|
| API calls and AutoSupport | HTTPS | 443 | Outbound internet and ONTAP cluster management LIF | API calls to GCP and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |
| DNS | UDP | 53 | DNS | Used for DNS resolve by Cloud Manager |

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.

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.

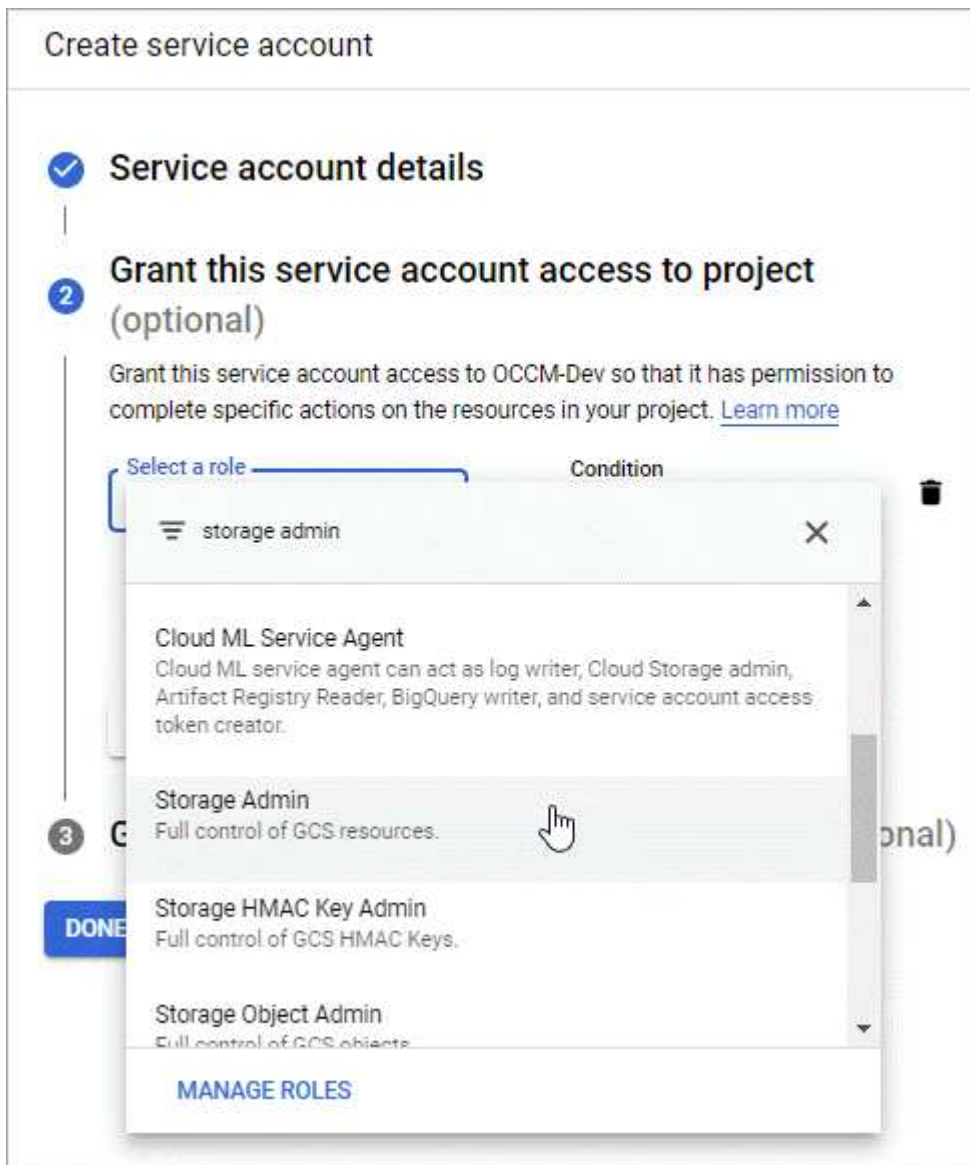
Cloud Volumes ONTAP uses the service account to access and manage one bucket for tiered data and another bucket for backups.

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.



- 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

gcp-sub2

Google Cloud Project

Marketplace Subscription

Edit Project

Details

Credentials

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account ⓘ

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

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 at the project level, in the project where the key is stored.

The permissions are provided in the [Connector 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, Cloud Manager 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 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.

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 working environment.

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. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Cloud Manager, select **Freemium** when you reach the charging methods page.

Select Charging Method

| | | | |
|----------------------------------|--------------------------|-------------|---|
| <input type="radio"/> | Professional | By capacity | ▼ |
| <input type="radio"/> | Essential | By capacity | ▼ |
| <input checked="" type="radio"/> | Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> | Per Node | By node | ▼ |

[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 package or the Professional package.

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

- A 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.

Steps

1. [Contact NetApp Sales to obtain a license](#)
2. [Add your NetApp Support Site account to Cloud Manager](#)

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

Your license must be available from the Digital Wallet before you can use it with Cloud Volumes ONTAP. If needed, you can [manually add the license to the Digital Wallet](#).

3. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Cloud Manager, select a capacity-based package when you reach the charging methods page.

| Select Charging Method | |
|--|-------------|
| <input checked="" type="radio"/> Professional | By capacity |
| <input type="radio"/> Essential | By capacity |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity |
| <input type="radio"/> Per Node | By node |

[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 working environment, Cloud Manager prompts you to subscribe to the agreement that's available in the Google Cloud Marketplace. That subscription is then associated with the working environment for charging. You can use that same subscription for additional working environments.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Cloud Manager, select a capacity-based package when you reach the charging methods page.

Select Charging Method

| | |
|--|----------------------------|
| <input checked="" type="radio"/> Professional | By capacity ▼ |
| <input type="radio"/> Essential | By capacity ▼ |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity ▼ |
| <input type="radio"/> Per Node | By node ▼ |

[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 working environment creation.

2. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - 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 Cloud Manager, select a capacity-based package when you reach the charging methods page.

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

[View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.](#)

Keystone Flex Subscription

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. [Learn more about Keystone Flex Subscriptions.](#)

Steps

1. If you don't have a subscription yet, [contact NetApp](#)
2. [Contact NetApp](#) to authorize your Cloud Manager user account with one or more Keystone Flex Subscriptions.
3. After NetApp authorizes your account, [link your subscriptions for use with Cloud Volumes ONTAP](#).
4. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.
 - a. Select the Keystone Flex Subscription charging method when prompted to choose a charging method.

Select Charging Method

☒

Keystone

By capacity

^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

☐

Professional

By capacity

v

☐

Essential

By capacity

v

☐

Freemium (Up to 500 GiB)

By capacity

v

☐

Per Node

By node

v

[View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.](#)

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 required 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 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

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. |
| Service Account Name | If you plan to use data tiering or Cloud Backup 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 . |
| 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 Google Cloud Documentation: Labeling Resources.</p> |
| 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 System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name. |

| Field | Description |
|--------------|---|
| 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, as described on this page.</p> </div> <p>Click Add Subscription 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. Alternatively, follow the steps to subscribe located in the [Associating a Marketplace subscription with GCP credentials](#) section.

► https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4

(video)

5. **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.
6. **Location & Connectivity:** Select a location, 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 Cloud Manager generate the firewall policy for you, you need to choose how you'll allow traffic: <ul style="list-style-type: none">• 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 Connector resides. This is the recommended option.• 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 . |

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 licensing options for Cloud Volumes ONTAP](#).
 - [Learn how to set up licensing](#).
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 and select a machine type.



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 9.10.1 and 9.10.1 P4 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 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**.

[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, Cloud Manager 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) | <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 bus 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, use the IQN to connect to the LUN from your hosts.</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 | <p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p> <p>If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.</p> |
| 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 | <p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter OU=Computers,OU=Cloud in this field.</p> <p>Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</p> |
| 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 | <p>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. See the Cloud Manager automation docs for details.</p> <p>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.</p> |

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 Tiering or Cloud Backup services, you need to enable the Service Account 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 Google Cloud Documentation: Labeling Resources.</p> |
| 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 System Manager or its CLI. Keep the default <i>admin</i> user name or change it to a custom user name. |

| Field | Description |
|--------------|---|
| 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, as described on this page.</p> </div> <p>Click Add Subscription 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. Alternatively, follow the steps to subscribe located in the [Associating a Marketplace subscription with GCP credentials](#) section.

► https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4

(video)

4. **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.
5. **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.](#)

6. **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 | <p>If you let Cloud Manager generate the firewall policy for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none">• 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 Connector resides. This is the recommended option.• If you choose All VPCs, the source filter for inbound traffic is the 0.0.0.0/0 IP range. |
| Use existing | <p>If you use an existing firewall policy, ensure that it includes the required rules.</p> <p>Learn about firewall rules for Cloud Volumes ONTAP.</p> |

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 licensing options for Cloud Volumes ONTAP.](#)
 - [Learn how to set up licensing.](#)
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 and select a machine type.



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 9.10.1 and 9.10.1 P4 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. **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**.

[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, 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. |

| Field | Description |
|--|--|
| 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 bus 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, use the IQN to connect to the LUN from your hosts.</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 | <p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p> <p>If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.</p> |
| Active Directory Domain to join | The FQDN of the Active Directory (AD) domain that you want the CIFS server to join. |

| Field | Description |
|---|--|
| 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 | <p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter OU=Computers,OU=Cloud in this field.</p> <p>Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</p> |
| 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 | <p>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. See the Cloud Manager automation docs for details.</p> <p>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.</p> |

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.

Copyright Information

Copyright © 2022 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.